ForeView™ Network Management User’s Manual

MANU0147-03 May, 1998

Software Version 4.3.x

FORE Systems, Inc.

1000 FORE Drive
Warrendale, PA 15086-7502
Phone: 412-742-4444
FAX: 412-742-7742

http://www.fore.com

Legal Notices

U.S. Government Restricted Rights. If you are licensing the Software on behalf of the U.S. Government (“Government”), the following provisions apply to you. If the Software is supplied to the Department of Defense (“DoD”), it is classified as “Commercial Computer Software” under paragraph 252.227-7014 of the DoD Supplement to the Federal Acquisition Regulations (“DFARS”) (or any successor regulations) and the Government is acquiring only the license rights granted herein (the license rights customarily provided to non-Government users). If the Software is supplied to any unit or agency of the Government other than DoD, it is classified as “Restricted Computer Software” and the Government’s rights in the Software are defined in paragraph 52.227-19 of the Federal Acquisition Regulations (“FAR”) (or any successor regulations) or, in the cases of NASA, in paragraph 18.52.227-86 of the NASA Supplement to the FAR (or any successor regulations).

Printed in the USA.

This publication is provided by FORE Systems, Inc. “as-is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties or conditions of merchantability or fitness for a particular purpose. FORE Systems, Inc. shall not be liable for any errors or omissions which may occur in this publication, nor for incidental or consequential damages of any kind resulting from the furnishing, performance, or use of this publication.

Information published here is current or planned as of the date of publication of this document. Because we are improving and adding features to our products continuously, the information in this document is subject to change without notice.

RESTRICTED RIGHTS LEGEND. Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 (October 1988) and FAR 52.227-19 (June 1987).

Preface

Chapter Summaries. xiii
Technical Support xv
Typographical Styles xvi
Important Information Indicators xvii

CHAPTER 1 Introduction

1.1 Capabilities of ForeView . . . . 1 - 2
1.2 ForeView Tools . . . . 1 - 3
1.3 Integration with Network Management Systems . . . . 1 - 5
1.3.1 HP OpenView and NetView for AIX . . . . 1 - 5
1.3.1.1 A Note About NetView for AIX. . . . . 1 - 5
1.3.2 SunNet Manager . . . . 1 - 7
1.4 Discovery and Topology Mapping. . . . . 1 - 8
1.5 On-line Help . . . . 1 - 9
1.6 Automatic Error Tracking. . . . . 1 - 10
1.7 Unpacking Information . . . . 1 - 11
1.8 System Requirements . . . . 1 - 12
1.8.1 Hardware . . . . 1 - 12
1.8.2 Software . . . . 1 - 13

CHAPTER 2 Software Installation

2.1 Obtaining the Software Distribution . . . . 2 - 2
2.1.1 Obtaining the Software Distribution via FTP. . . . . 2 - 2
2.2 Re-installation Procedure . . . . 2 - 4
2.3 Before You Begin . . . . 2 - 6
2.3.1 Software License Key. . . . . 2 - 6
2.3.2 Installation Requirements for Partitioning the Network. . . . . 2 - 6
2.4 Installation from FTP File . . . . 2 - 7
2.4.1 Software Installation . . . . 2 - 7
2.5 Installation from CD-ROM. . . . . 2 - 8
2.5.1 UNIX Platform . . . . 2 - 8
2.5.2 Software Installation in an Alternate Directory . . . . 2 - 8
2.5.3 Windows NT Installation. . . . . 2 - 10
2.5.4 Import the Host Name File . . . . 2 - 11

CHAPTER 3 Configuring ForeView

3.1 Overview. . . . . 3 - 1
3.1.1 General Format . . . . 3 - 2
3.1.2 Discovery Server . . . . 3 - 2

3.1.3 Alternate Discovery . . . . 3 - 3
3.1.4 Stand-alone Map Display Order . . . . 3 - 4
3.1.5 Stand-alone Map NNIs . . . . 3 - 4
3.1.6 Graph Type . . . . 3 - 5
3.1.7 Maximum Points to Display . . . . 3 - 5
3.1.8 Displaying Reserved Channels . . . . 3 - 5
3.1.9 Status Polling. . . . . 3 - 5
3.1.10 Enclosure Identification Name Mapping . . . . 3 - 6

3.2 Configuring SNMP. . . . . 3 - 7

3.2.1 Aligning SNMP Configuration with HP OpenView SNMP Configuration 3 - 7
3.2.2 Community Names . . . . 3 - 7

3.3 Advanced Configuration . . . . 3 - 8

3.3.1 Host Interface Preferences Configuration . . . . 3 - 8
3.3.1.1 User Preferences . . . . 3 - 9
3.3.1.2 Specifying User Preferences . . . . 3 - 10
3.3.2 Link Status Propagation . . . . 3 - 11
3.3.3 Port Management Status Configuration . . . . 3 - 11
3.3.4 Distributed Discovery. . . . . 3 - 11
3.3.5 Adding New Devices . . . . 3 - 12
3.3.5.1 How to use the FvAccess Mechanism . . . . 3 - 13
3.3.5.2 Handling Non-IP, ATM-connected Devices . . . . 3 - 13
3.3.5.3 Learning IP Addresses of Connected Devices. . . . . 3 - 14
3.3.5.4 Additional Installation Instructions . . . . 3 - 14
3.3.5.4.1 Front Panel . . . . 3 - 14
3.3.5.4.2 Stand-alone Map . . . . 3 - 15
3.3.5.4.3 SunNet Manager Discovery. . . . . 3 - 15
3.3.5.5 FV-OV Processes . . . . 3 - 16

3.4 Configuration Template . . . . 3 - 18

CHAPTER 4 Network Discovery

4.1 How the Discovery and Status Server Works . . . . 4 - 2

4.1.1 Discovery Arguments . . . . 4 - 2
4.1.2 Polling Arguments . . . . 4 - 3
4.1.3 Seeding the Discovery. . . . . 4 - 4
4.1.4 Limiting the Discovery and Polling. . . . . 4 - 4
4.1.4.1 Customized Discovery and Polling . . . . 4 - 5
4.1.5 Configuration File Resources . . . . 4 - 6
4.1.6 Alternative Discovery Mode. . . . . 4 - 7

4.2 Scaling Network Discovery . . . . 4 - 8

4.2.1 How Scaling Works with OpenView/NetView . . . . 4 - 8
4.2.2 How Scaling Works with the Stand-alone Map . . . . 4 - 9
4.2.3 How To Deploy Scaling . . . . 4 - 10

4.2.4 Monitoring Edge Switches . . . . .4 - 10
4.2.5 Enabling Scaling. . . . . .4 - 12

CHAPTER 5 Running ForeView with HP OpenView and NetView for AIX

5.1 Starting ForeView with OpenView/NetView . . . . .5 - 2
5.1.1 Installation Note for AIX 4.1 with NetView 4.x .5 - 2
5.2 The Discovery Process. . . . . .5 - 3
5.2.1 Polling Network Elements. . . . . .5 - 3
5.3 ForeView's ATM Map . . . . .5 - 4
5.3.1 Root Level Submap . . . . .5 - 4
5.3.2 ATM Networks Submap . . . . .5 - 5
5.3.3 Switch Connections Submap . . . . .5 - 6
5.3.4 ATM Links Submap . . . . .5 - 7
5.3.5 Link Information Submap . . . . .5 - 8
5.3.6 Fabrics Submap . . . . .5 - 9
5.3.7 How Status Colors are Derived . . . . .5 - 9
5.3.8 Location Symbols . . . . .5 - 10
5.3.8.1 How Location Symbols are Implemented . . . . .5 - 11
5.3.8.2 Implementation Summary . . . . .5 - 12
5.3.8.2.1 Start-up. . . . . .5 - 12
5.3.8.2.2 Symbol Deletion . . . . .5 - 12
5.3.8.2.3 Symbol Creation . . . . .5 - 12
5.4 Map Icons . . . . .5 - 13
5.4.1 ATM Switches. . . . . .5 - 13
5.4.2 Hosts . . . . .5 - 13
5.5 The Discovery Process. . . . . .5 - 14
5.5.1 Polling Network Elements. . . . . .5 - 14
5.5.2 SNMP Traps . . . . .5 - 15
5.6 Launching ForeView Tools from HP Openview. . . . . .5 - 16
5.6.1 Selecting ATM Devices and Hosts . . . . .5 - 16
5.6.2 ForeView Tools. . . . . .5 - 16
5.6.3 Selection Options for Graphing and Logging . . . . .5 - 17
5.7 Threshold Events and Actions with HP OpenView Network Node Manager . . . .5 - 20
5.7.1 Setting Up a Threshold Event. . . . . .5 - 20
5.7.2 Summary of Setting Up a Threshold Event . . . . .5 - 20
5.7.3 Select a MIB Variable to Monitor . . . . .5 - 20
5.7.4 Set Up Event Thresholds . . . . .5 - 23
5.7.5 Set Up an Action On a Threshold Event. . . . . .5 - 24
5.8 Debugging Threshold Events . . . . .5 - 27
5.9 Trap Configuration . . . . .5 - 28
5.9.1 Changing Trap Severity . . . . .5 - 28

5.10 Troubleshooting ForeView on HP OpenView . . . . . 5 - 30
5.10.1 Checking ForeView Processes . . . . . 5 - 30
5.10.2 Checking Error Logs . . . . . 5 - 30
5.10.3 Examining the OVW Database . . . . . 5 - 31
5.10.4 Deleting the Map Database and Rediscovering . . . . . 5 - 31
5.10.5 Creating a Trap Category . . . . . 5 - 33
5.11 Maintenance Commands . . . . . 5 - 34
5.11.1 Options for fvovmap . . . . . 5 - 34
5.11.1.1 Options . . . . . 5 - 35
5.11.1.2 Files . . . . . 5 - 35
5.11.2 Options for Status and Monitoring . . . . . 5 - 35
5.11.3 Options for Handling FORE-specific Traps . . . . . 5 - 38
5.11.4 Unmanaging Objects in the HP OpenView Database . . . . . 5 - 40

CHAPTER 6 Running ForeView with SunNet Manager

6.1 Starting ForeView with SunNet Manager . . . . . 6 - 2
6.1.1 Starting the Discovery and Status Daemon . . . . . 6 - 2
6.1.2 Initializing the SunNet Manager Database . . . . . 6 - 3
6.1.3 Running the Discovery Tool . . . . . 6 - 4
6.2 SunNet Manager's Home View . . . . . 6 - 5
6.3 ATM Networks View . . . . . 6 - 6
6.3.1 Interswitch Links . . . . . 6 - 7
6.3.2 Switch Subnet Glyphs . . . . . 6 - 7
6.4 Switch Connections View . . . . . 6 - 8
6.4.1 ATM Switch, Host, and LAN-access Device Labels . . . . . 6 - 9
6.4.2 Optional Method for Discovery . . . . . 6 - 9
6.5 Launching ForeView Tools from SunNet Manager . . . . . 6 - 11
6.5.1 Activating ForeView Tools from the Console . . . . . 6 - 11
6.5.2 Activating ForeView Tools from a Glyph . . . . . 6 - 12
6.6 ATM Network Status . . . . . 6 - 15
6.7 Monitoring the ATM Network . . . . . 6 - 16
6.7.1 SNMP Traps . . . . . 6 - 17
6.7.2 Update Properties . . . . . 6 - 17
6.8 Re-discovering the Network . . . . . 6 - 18
6.9 Troubleshooting ForeView on SunNet Manager . . . . . 6 - 19
6.9.1 Problems with Discovery . . . . . 6 - 19
6.9.2 Problems Receiving Traps . . . . . 6 - 19
6.9.3 Error Logs . . . . . 6 - 19

CHAPTER 7 Running ForeView's Stand-alone Map

7.1 Starting the Stand-alone Map . . . . . 7 - 2

7.1.1 Limiting Network Discovery . . . . 7 - 2

7.2 Viewing Options for the Stand-alone Map . . . . 7 - 4

7.2.1 Launching a Connection Submap . . . . 7 - 5

7.3 Menus. . . . . 7 - 6

7.3.1 File . . . . 7 - 6

7.3.2 Edit . . . . 7 - 6

7.3.3 Tools . . . . 7 - 6

7.3.4 Select . . . . 7 - 8

7.3.5 Options . . . . 7 - 8

7.3.6 Help . . . . 7 - 8

7.4 Navigating the Map. . . . . 7 - 9

CHAPTER 8 Front Panel

8.1 ATM Backbone Switches . . . . 8 - 2

8.1.1 ASX-1000 . . . . 8 - 2

8.1.2 ASX-200BX . . . . 8 - 3

8.1.3 MSC-900 . . . . 8 - 3

8.1.4 TNX-210 . . . . 8 - 4

8.1.5 TNX-1100 . . . . 8 - 4

8.2 ATM Workgroup Switches. . . . . 8 - 5

8.3 Switch Control Processors . . . . 8 - 7

8.3.1 SPARC RISC Switch Control Processor. . . . . 8 - 7

8.3.2 i960 Switch Control Processor . . . . 8 - 7

8.4 Network Modules . . . . 8 - 8

8.4.1 Port Numbering . . . . 8 - 8

8.5 Port Indicators . . . . 8 - 9

8.6 Menu Bar . . . . 8 - 11

8.6.1 File . . . . 8 - 11

8.6.2 Edit . . . . 8 - 11

8.6.3 Configure . . . . 8 - 11

8.6.4 Tachometers. . . . . 8 - 12

8.6.5 Polling. . . . . 8 - 13

8.6.6 VCC/VPC Control. . . . . 8 - 14

8.6.7 System . . . . 8 - 14

8.6.8 Help . . . . 8 - 14

8.7 Configuring and Monitoring Ports. . . . . 8 - 15

8.8 Generic Port Configuration. . . . . 8 - 16

8.8.1 Port Status . . . . 8 - 16

8.8.2 Port Control . . . . 8 - 17

8.8.3 Port Statistics--Activity . . . . 8 - 17

8.8.4 Port Statistics--Capacity . . . . 8 - 18
8.8.4.1 Port Statistics--Input Capacity . . . . 8 - 18
8.8.4.2 Port Statistics--Output Capacity . . . . 8 - 18
8.8.5 Port Statistics--Errors . . . . 8 - 19
8.9 LED Mode Port Configuration . . . . 8 - 21
8.10 Configuring and Monitoring OC-3 and OC-12
(SONET) Ports8 - 23
8.10.1 Port Control . . . . 8 - 23
8.10.2 OCx Status . . . . 8 - 24
8.10.3 OCx Statistics . . . . 8 - 26
8.10.3.1 Section . . . . 8 - 26
8.10.3.2 Path . . . . 8 - 27
8.10.3.3 Header Check. . . . . 8 - 28
8.11 Configuring and Monitoring DS-3 Ports. . . . . 8 - 29
8.11.1 Port Control . . . . 8 - 30
8.11.2 DS-3 Status . . . . 8 - 31
8.11.3 DS-3 Statistics. . . . . 8 - 32
8.11.3.1 Framing. . . . . 8 - 32
8.11.3.2 PLCP . . . . 8 - 33
8.12 Configuring and Monitoring DS-1 Ports. . . . . 8 - 34
8.12.1 Port Control . . . . 8 - 35
8.12.2 DS-1 Status . . . . 8 - 36
8.12.3 DS-1 Statistics. . . . . 8 - 37
8.12.3.1 Framing. . . . . 8 - 37
8.12.3.2 ATM . . . . 8 - 37
8.13 Configuring and Monitoring E-3 Ports . . . . 8 - 38
8.13.1 Port Control . . . . 8 - 39
8.13.2 E-3 Status . . . . 8 - 40
8.13.3 E-3 Statistics . . . . 8 - 41
8.13.3.1 Framing. . . . . 8 - 41
8.13.3.2 PLCP . . . . 8 - 41
8.14 Configuring and Monitoring E-1 Ports . . . . 8 - 43
8.14.1 Port Control . . . . 8 - 44
8.14.2 Port Status. . . . . 8 - 45
8.14.3 E-1 Statistics . . . . 8 - 46
8.14.3.1 Framing. . . . . 8 - 46
8.14.3.2 ATM . . . . 8 - 47
8.15 Configuring and Monitoring J-2 Ports . . . . 8 - 48
8.15.1 Port Control . . . . 8 - 49
8.15.2 J-2 Status . . . . 8 - 49
8.15.3 J-2 Statistics . . . . 8 - 50

8.15.3.1 Errors . . . . . 8 - 50
8.15.3.2 ATM . . . . . 8 - 50

8.16 Configuring and Monitoring TP-25 Ports . . . . . 8 - 51

8.16.1 Port Control . . . . . 8 - 51
8.16.2 TP-25 Status . . . . . 8 - 52
8.16.3 TP-25 Statistics . . . . . 8 - 52
8.16.3.1 ATM . . . . . 8 - 52

8.17 Configuring and Monitoring CEMDS1 Ports . . . . . 8 - 53

8.17.1 CEMDS1 Port Control . . . . . 8 - 53
8.17.2 CEMDS1 Status . . . . . 8 - 54
8.17.3 CEMDS1 Statistics . . . . . 8 - 55
8.17.3.1 DSx1 Line . . . . . 8 - 55
8.17.3.2 Framing . . . . . 8 - 55
8.17.3.3 ATM . . . . . 8 - 56

8.18 Configuring and Monitoring CEME1 Ports . . . . . 8 - 57

8.18.1 CEME1 Port Control . . . . . 8 - 57
8.18.2 CEME1 Status . . . . . 8 - 58
8.18.3 CEME1 Statistics . . . . . 8 - 59
8.18.3.1 E1 Line . . . . . 8 - 59
8.18.3.2 Framing . . . . . 8 - 59
8.18.3.3 ATM . . . . . 8 - 60

8.19 Configuring Port Level Traffic . . . . . 8 - 61

8.19.1 Series D Network Modules . . . . . 8 - 61
8.19.2 Series C Network Modules . . . . . 8 - 61
8.19.3 Series LC Network Modules . . . . . 8 - 64

8.20 Configuring Port Level CAC . . . . . 8 - 66

8.21 OAM Management . . . . . 8 - 67

8.22 Configuring and Monitoring Network Modules . . . . . 8 - 68

8.23 Configuring Timing . . . . . 8 - 69

8.23.1 Advanced Timing . . . . . 8 - 70

8.24 Configuring IP . . . . . 8 - 72

8.25 Configuring IP Interfaces . . . . . 8 - 73

8.25.1 Modifying an IP Interface . . . . . 8 - 74

8.26 Configuring IP Routing . . . . . 8 - 76

8.26.1 Adding an IP Route . . . . . 8 - 77

8.27 Configuring Signalling. . . . . . 8 - 78

8.27.1 Signalling Information . . . . . 8 - 79
8.27.1.1 SPANS Information . . . . . 8 - 79
8.27.1.2 UNI 3.x Information . . . . . 8 - 80

8.28 Alarm Control . . . . . 8 - 81

8.29 Configuring ATM Connection Routing . . . . 8 - 83
8.30 Configuring NSAP Routing . . . . 8 - 84
8.30.1 Prefixes . . . . 8 - 84
8.30.1.1 ICD . . . . 8 - 84
8.30.1.2 DCC . . . . 8 - 85
8.30.1.3 E.164 . . . . 8 - 85
8.30.2 Static Routing . . . . 8 - 86
8.30.2.1 ICD . . . . 8 - 86
8.30.2.2 DCC . . . . 8 - 87
8.30.2.3 E.164 . . . . 8 - 87
8.30.3 Show ILMI . . . . 8 - 88
8.31 Models . . . . 8 - 89
8.32 Address Validation . . . . 8 - 91
8.33 PMP Configuration. . . . . 8 - 92
8.34 PNNI-SPVC Pace and Reroute Configuration . . . . 8 - 93
8.34.1 Pacing . . . . 8 - 93
8.34.2 Rerouting . . . . 8 - 93
8.35 SCP Configuration . . . . 8 - 96
8.35.1 Dual SCP Configuration Menu . . . . 8 - 97
8.35.1.1 SCP Control . . . . 8 - 98
8.35.1.2 SCP Status . . . . 8 - 99
8.35.1.3 Synchronization Statistics. . . . . 8 - 100
8.35.2 SCP Synchronization Request . . . . 8 - 100
8.35.3 Switching over to the Standby SCP. . . . . 8 - 102
8.35.4 Resetting the Standby SCP. . . . . 8 - 102

CHAPTER 9 Connection Management

9.1 The Virtual Path/Channel Tool . . . . 9 - 3
9.1.1 Tool Type . . . . 9 - 4
9.1.2 Channel Control . . . . 9 - 4
9.1.3 Command Buttons. . . . . 9 - 5
9.1.3.1 Command Button Modes . . . . 9 - 6
9.2 Tool Options. . . . . 9 - 8
9.2.1 Filtering by Path and Channel Type. . . . . 9 - 9
9.2.2 Enabling Configuration of UPC Contracts . . . . 9 - 10
9.2.3 Showing P-MP and MP-P Confirmation Dialog Boxes . . . . 9 - 10
9.2.4 Showing Confirmation Dialog Boxes . . . . 9 - 10
9.2.5 Sorting Criteria . . . . 9 - 10
9.2.6 Display Columns . . . . 9 - 11
9.2.6.1 Moving Columns. . . . . 9 - 11
9.3 Creating Smart PVCs . . . . 9 - 12

9.3.1 Key Fields for the Smart PVC Tool . . . . 9 - 13
9.3.2 Optional Fields for the Smart PVC Tool . . . . 9 - 13
9.3.3 CES Configuration for Smart PVCs . . . . 9 - 14
9.4 PVC Tool. . . . . 9 - 16
9.4.1 Key Fields for the PVC Tool . . . . 9 - 16
9.4.2 Optional Fields for the PVC Tool . . . . 9 - 17
9.5 PVP Tool. . . . . 9 - 19
9.5.1 Key Fields for the PVP Tool . . . . 9 - 19
9.5.2 Optional Fields for the PVP Tool. . . . . 9 - 20
9.6 PNNI SPVC Tool. . . . . 9 - 21
9.6.1 Key Fields for the PNNI SPVC Tool . . . . 9 - 21
9.6.2 Optional Fields for the PNNI SPVC Tool . . . . 9 - 22
9.7 Incoming Path Tool . . . . 9 - 24
9.7.1 Key Fields for the Incoming Path Tool . . . . 9 - 25
9.7.2 Optional Fields for the Incoming Path Tool . . . . 9 - 25
9.8 Outgoing Path Tool . . . . 9 - 26
9.8.1 Key Fields for the Outgoing Path Tool . . . . 9 - 27
9.8.2 Optional Fields for the Incoming Path Tool . . . . 9 - 27
9.9 Signalling Path Tool . . . . 9 - 29
9.9.1 SPANS Configuration . . . . 9 - 30
9.9.1.1 Key Fields for the SPANS Signalling Path Tool . . . . 9 - 30
9.9.1.2 Optional Fields for the SPANS Signalling Path Tool . . . . 9 - 31
9.9.2 UNI 3.x Configuration . . . . 9 - 32
9.9.2.1 Key Fields for the UNI 3.x Path Tool . . . . 9 - 33
9.9.2.2 Optional Fields for the UNI 3.x Path Tool. . . . . 9 - 33
9.9.3 UNI 3.x Signalling Configuration . . . . 9 - 35
9.9.3.1 Key Fields for the UNI 3.x Signalling Path Tool . . . . 9 - 35
9.9.4 UNI 3.x ILMI Signalling Configuration . . . . 9 - 37
9.9.4.1 Key Fields for the UNI 3.x ILMI Path Tool . . . . 9 - 37
9.9.5 UNI 3.x Address Validation. . . . . 9 - 38
9.9.5.1 Key Fields for UNI 3.x Signalling Address Validation . . . . 9 - 38
9.9.6 UNI 3.x Address Mapping . . . . 9 - 40
9.9.6.1 Key Fields for UNI 3.x E.164 Address Mapping . . . . 9 - 40
9.10 Usage Parameter Control (UPC) Contracts . . . . 9 - 41
9.10.1 Traffic Types . . . . 9 - 41
9.10.2 Detailed UPC Reference . . . . 9 - 45
9.11 General Concepts of UPC Contracts . . . . 9 - 47
9.11.1 Setting the CLP Bit . . . . 9 - 47
9.11.2 Leaky Bucket Algorithm . . . . 9 - 47
9.11.3 UNI 3.x UPC Traffic Contract Parameters . . . . 9 - 48

CHAPTER 10 Tracking Network Usage

10.1 Graphing Network Usage Overview . . . . 10 - 2
10.1.1 The Graph Tools . . . . 10 - 2
10.1.2 Selection Options . . . . 10 - 3
10.1.2.1 Graphing Switch Options Summary . . . . 10 - 3
10.1.2.2 Graphing Host Options Summary . . . . 10 - 3
10.1.3 Graphing Example. . . . . 10 - 5
10.2 Logging Network Usage Overview . . . . 10 - 8
10.2.1 The Log Tools . . . . 10 - 8
10.2.2 Selection Options . . . . 10 - 8
10.2.2.1 Logging Switch Options Summary . . . . 10 - 9
10.2.2.2 Logging Host Options Summary . . . . 10 - 9
10.2.3 Logging Example. . . . . 10 - 10
10.3 Billing for Network Usage . . . . 10 - 15
10.4 Graphing and Logging from the Command-line. . . . . 10 - 18

CHAPTER 11 Channel and Path Tracing

11.1 Uses for the Channel/Path Tracer . . . . 11 - 2
11.2 Tracing Channels and Paths in a Network. . . . . 11 - 3
11.2.1 Selecting Links and Switches for Tracing . . . . 11 - 3
11.2.2 Tabular Traces . . . . 11 - 4
11.2.3 Graphing Traces . . . . 11 - 6
11.2.4 Point-to-Multipoint Traces . . . . 11 - 10
11.2.5 Multipoint-to-Point Traces . . . . 11 - 12
11.2.6 Tracing Through a PVP . . . . 11 - 15
11.3 Tracing from the Command-line. . . . . 11 - 17

CHAPTER 12 Taking Inventory of ATM Equipment

12.1 Launching the Inventory Utility. . . . . 12 - 1
12.1.1 Defining the Version History File . . . . 12 - 2
12.2 The Inventory Dialog . . . . 12 - 3
12.2.1 Inventory Options . . . . 12 - 3
12.3 Filtering . . . . 12 - 4
12.3.1 Filtering by Device or Host Type . . . . 12 - 5
12.3.2 Filtering by Names and Versions. . . . . 12 - 5
12.4 Sorting . . . . 12 - 6
12.4.1 Sort Order . . . . 12 - 6
12.4.2 Moving Columns . . . . 12 - 7
12.5 Version History . . . . 12 - 8
12.6 Inventory from the Command-line . . . . 12 - 8

CHAPTER 13 OAM Management

13.1 Introduction . . . . 13 - 1
13.2 OAM Capabilities . . . . 13 - 4
13.2.1 OAM Cell Generation Activation . . . . 13 - 4
13.2.2 OAM Switch Monitor . . . . 13 - 5
13.2.3 Menu Bar . . . . 13 - 7
13.2.3.1 File . . . . 13 - 7
13.2.3.2 Data . . . . 13 - 7
13.2.3.3 Help . . . . 13 - 8
13.3 OAM Monitoring from the Command-line . . . . 13 - 8

CHAPTER 14 Call Record and Performance Monitoring

14.1 General Functionality . . . . 14 - 1
14.1.1 Call Record Data Collection . . . . 14 - 2
14.1.2 Performance Monitoring Data Collection . . . . 14 - 3
14.2 The Call and Performance Record Configuration Interface . . . . 14 - 4
14.2.1 Synchronizing Switch Time . . . . 14 - 8
14.3 Post Processing of Records . . . . 14 - 9
14.3.1 Record Output . . . . 14 - 9
14.3.2 Call Record Data . . . . 14 - 10
14.3.3 Performance Record Data . . . . 14 - 10
14.4 Call Record and Performance Record Statistics . . . . 14 - 12
14.4.1 Call Record Statistics . . . . 14 - 12
14.4.2 Performance Record Statistics . . . . 14 - 14
14.5 Example Application . . . . 14 - 16
14.5.1 Post Processing of Records . . . . 14 - 18
14.6 Call Records from the Command-line . . . . 14 - 20

CHAPTER 15 Software Manager

15.1 Software Upgrades from the Command-line . . . . 15 - 4

CHAPTER 16 Remote Console Interface and Scripting with AMI

16.1 What Is AMI? . . . . 16 - 1
16.1.1 Where to Find More Information on AMI . . . . 16 - 2
16.2 Initial Login from Serial Port or Telnet . . . . 16 - 3
16.2.1 Login from Serial Port . . . . 16 - 3
16.2.2 Login from Telnet . . . . 16 - 4
16.3 AMI Commands Not Available When Running Remotely . . . . 16 - 6
16.4 PNNI Topology Configuration Commands . . . . 16 - 8
16.4.1 ForeThought PNNI Configuration Commands . . . . 16 - 8

16.4.1.1 Setting the ForeThought PNNI Switch Prefix . . . . 16 - 8
16.4.1.2 Changing the ForeThought PNNI Border Switch Functionality 16 - 9
16.4.1.3 Setting the ForeThought PNNI Switch Prefix Mask . . . . 16 - 9
16.4.1.4 Setting the ForeThought PNNI Peergroup Mask . . . . 16 - 10
16.4.1.5 Setting the Hello Indication Interval . . . . 16 - 10
16.4.1.6 Setting the NSAP Indication Interval . . . . 16 - 10
16.4.1.7 Setting the Static Route Update Indication Interval . . . . 16 - 11
16.4.1.8 Setting the Maximum Hop Count . . . . 16 - 11
16.4.1.9 Setting the Proportional Multiplier . . . . 16 - 11
16.4.1.10 Setting a Minimum Threshold for NSAP Updates . . . . 16 - 12
16.4.1.11 Setting a Minimum Virtual Channel Mark . . . . 16 - 12
16.4.1.12 Displaying ForeThought PNNI Parameters . . . . 16 - 12
16.4.2 Topology Scripts . . . . 16 - 14
16.4.2.1 PNNI Topology Script . . . . 16 - 14
16.4.2.2 SPANS Topology Script . . . . 16 - 15
16.5 Example Scripts. . . . . 16 - 16
16.5.1 Retrieving Switch Information . . . . 16 - 16
16.5.2 Creating a PVC . . . . 16 - 17
16.5.3 Creating a Broadcast using PVCs. . . . . 16 - 18

APPENDIX A An Overview of Virtual Connections

A.1 General Concepts . . . . A - 1
A.2 Virtual Paths . . . . A - 3
A.2.1 Through Paths (PVPs). . . . . A - 4
A.2.2 Outgoing and Incoming Paths . . . . A - 6
A.3 Virtual Channels . . . . A - 7
A.4 Smart PVCs. . . . . A - 10

APPENDIX B Channel Usage in FORE ATM Networks

B.1 Signalling Channels and Reserved Paths . . . . B - 1

APPENDIX C SNMP Indexing

APPENDIX D SNMP Traps

Acronyms

Glossary

Index

Preface

The intent of this manual is to supply users of the *ForeView*^{TM} Network Management software with all the necessary information to successfully install and operate the *ForeView* software package. This document was created for users with various levels of experience. If you have any questions or problems with the installation, please contact FORE Systems' Technical Support.

Chapter Summaries

Chapter 1 - Introduction - Provides an overview of the *ForeView* Network Management package, a description of hardware and software requirements, and general information pertaining to the capabilities and features of the *ForeView* Network Management software package, including a new mechanism for reporting bugs to FORE Systems Technical Support (fvtaclnk).

Chapter 2 - Software Installation - Guides you through the installation of your *ForeView* Network Management software. Included are software installation instructions for *ForeView* running under HP OpenView, NetView for AIX, SunNet Manager, and the Stand-alone Map; and product registration information.

Chapter 3 - Configuring *ForeView* - Explains how to edit the *ForeView* configuration file as well as the configuration requirements for the various platforms.

Chapter 4 - Network Discovery - Explains how *ForeView* utilizes a discovery and status server application that discovers *ForeRunner* switches, NNI and UNI links, and the endpoints of NNI and UNI links in an ATM network.

Chapter 5 - Running *ForeView* with HP OpenView and NetView for AIX - This chapter focuses on *ForeView* running under HP OpenView and NetView for AIX, and highlights the unique characteristics of network mapping, icons, and utilities.

Chapter 6 - Running *ForeView* with SunNet Manager - This chapter focuses on *ForeView* running under SunNet Manager and highlights the unique characteristics of network mapping, icons, and utilities.

Chapter 7 - Running *ForeView*'s Stand-alone Map - This chapter provides information on how to run the *ForeView* Stand-alone Map that runs independent of a network management system, as well as under the OpenWindows environment.

Chapter 8 - Front Panel - Graphically displays the front panel, all the indicators, and the conditions of a FORE Systems switch as displayed by *ForeView*.

Chapter 9 - Connection Management - Describes how to create and browse SPVCs, PVCs, Signalling Paths, and Through Paths using the Channel and Path tools within *ForeView*.

Chapter 10 - Tracking Network Usage - Discusses the utilities provided for tracking network usage. These utilities are fvgraph, the graph utility and fvlog, the logging utility.

Chapter 11 - Channel and Path Tracing - Discusses the tracing of channels and paths from end-to-end in network. These channel traces may be viewed in a tabular or graph format.

Chapter 12 - Taking Inventory of ATM Equipment - Discusses the graphical interface that displays the network inventory and the manipulation of the data via filters and sorting to present specific inventory displays.

Chapter 13 - OAM Management - Discusses *ForeView*'s use of OAM cells to provide a means to support fault and performance management at the ATM layer.

Chapter 14 - Call Record and Performance Monitoring - Discusses call record and performance monitoring data collection for billing and connection performance monitoring.

Chapter 15 - Software Manager - Discusses the graphical interface that facilitates upgrades of the software running on FORE ATM switches.

Chapter 16 - Remote Console Interface and Scripting with AMI - Discusses the *ForeRunner* ASX Management Interface (AMI) and includes several scripting examples.

Appendix A - An Overview of Virtual Connections - Explains the fundamentals of PVC configuration and usage.

Appendix B - Channel Usage in FORE ATM Networks - Explains which channels are used for signalling and which paths are reserved.

Appendix C - SNMP Indexing - Summarizes the two main SNMP indexing schemes used to index SNMP statistics: software port indices and hardware port indices.

Appendix D - SNMP Traps - Summarizes in tabular format the traps generated by FORE switches.

Technical Support

If your equipment is under warranty or a support contract with FORE Systems, please reference the following information for technical support issues.

In the U.S.A., you can contact FORE Systems' Technical Support by any one of four methods:

1. If you have access to Internet, you may contact FORE Systems' Technical Support via e-mail at the following address:

support@fore.com

1. You may FAX your questions to "support" at:

412-742-7900

2. You may send questions, via U S Mail, to the following address:

FORE Systems, Inc.
1000 FORE Drive
Warrendale, PA 15086-7502

3. You may telephone your questions to "support" at:

1-800-671-FORE (3673) or **412-635-3700**

Technical support for non-U.S.A. customers should be handled through your local distributor.

No matter which method is used for technical support, please be prepared to provide your support contract ID number, the serial number(s) of the product(s) and as much information as possible describing your problem or question.

Typographical Styles

Throughout this manual, specific commands to be entered by the user appear on a separate line in bold typeface. In addition, use of the `Enter` or `Return` key is represented as `<ENTER>`. The following example demonstrates this convention:

```
cd /usr <ENTER>
```

Commands or file names that appear within the text of this manual are represented in the following style: "...the **`fore_install`** program will install this distribution"

As in the following example, any messages appearing on your screen during software installation and network interface administration will appear in `Courier` font to distinguish them from the rest of the text.

```
.... Are all four conditions true?
```

Important Information Indicators

To call your attention to important information that must be reviewed to ensure correct and complete installation, as well as to avoid problems with your software, FORE Systems utilizes the following *CAUTION/NOTE* indicators.

Information contained in **CAUTION** statements is important for proper installation/operation. **CAUTION** statements can prevent possible equipment damage and/or loss of data and will be indicated as:

CAUTION ⚠

You risk damaging your equipment and/or software if you do not follow these instructions.

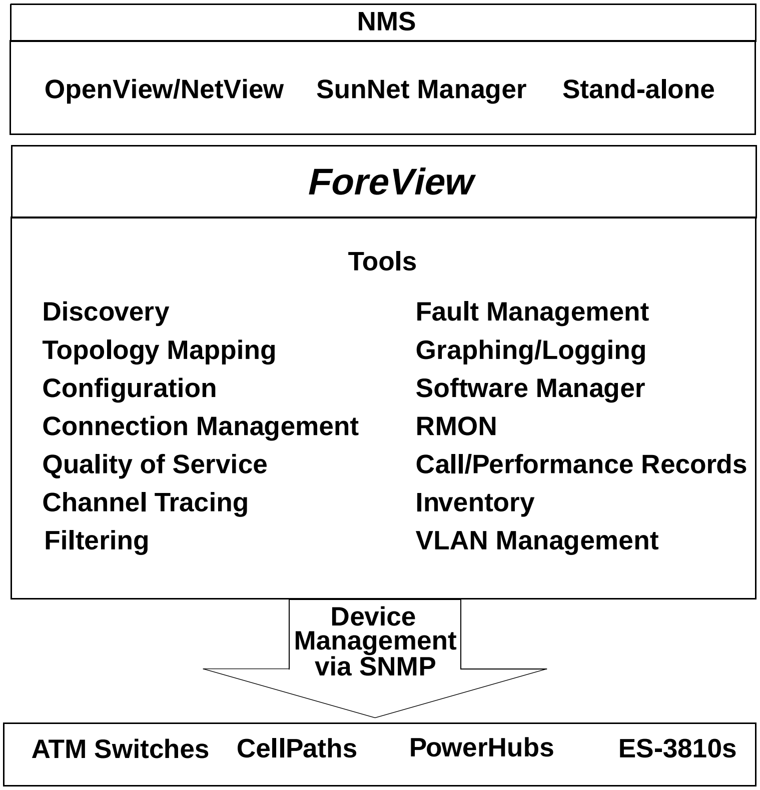
Information contained in **NOTE** statements has been found important enough to be called to the special attention of the operator and will be set off from the text as follows:

NOTE ➡

FORE Systems strongly recommends that you disconnect the serial cable once you have configured the *ForeRunner* switch and then access the *ForeRunner* switch over the ATM network.

CHAPTER 1 Introduction

ForeView™ Network Management from FORE Systems is a sophisticated management application for switched internetworks that integrates with HP OpenView, NetView for AIX, SunNet Manager, and Windows NT to provide a complete solution for managing FORE ATM networks. Although *ForeView* manages the ATM network using the IP protocol, it does not manage the IP network itself. Those tasks are left to the integrated Network Management Systems (NMSs) such as HP OpenView. *ForeView* is designed to work integrally with these IP NMSs, or to function as a stand-alone management system, to manage FORE Systems' devices.



1.1 Capabilities of *ForeView*

ForeView Network Management software provides a complete solution for managing FORE ATM networks in a variety of network environments. *ForeView* provides a quick visual assessment of the general state of FORE devices, as well as detailed examination of connection status, and diagnosis in the event of errors. *ForeView* is designed to operate under graphical environments including Sun OpenWindows, CDE, and Windows NT; and works under native operating systems such as Solaris, HP-UX, IRIX, AIX, and Windows NT. A list of supported hardware and software platforms can be found in “System Requirements” on page 1 - 12.

ForeView software is a set of components that allow a network manager to perform such functions as evaluate the ATM network topology, take inventory of ATM devices and software, implement device configuration and management, and track network usage via log files and graphing statistics. *ForeView* provides this base set of tools under each NMS and related operating system. In each instance, the tools have a unified “look and feel” that is consistent across platforms. A table describing the tools can be found in “ForeView Tools” on page 1 - 3.

When *ForeView* is installed in an environment that utilizes an NMS (HP OpenView or SunNet Manager, for example), the network manager can take advantage of some of the integrated features of the NMS, such as topology management, event logging, error trapping, graphing modules, and threshold programming. *ForeView* also can be installed as a stand-alone management application that provides its own topology map. In addition, the various management tools are also available in the stand-alone version. A summary of *ForeView*’s integration with NMSs can be found in “Integration with Network Management Systems” on page 1 - 5.

1.2 *ForeView* Tools

As previously mentioned, *ForeView* provides a base set of tools under each NMS and related operating system. These tools have a unified “look and feel” that is consistent across platforms. These tools allow you to monitor the ATM Network, take inventory of ATM equipment, create connections, and track network usage. You can also launch separate ATM Network maps. The tools are integrated into a **`ForeView`** menu within the NMS and can also be run outside of the NMS via the command line.

A summary of how these tools are accessed and launched from *ForeView*, either integrated with an NMS or stand-alone, can be found in section 1.3. The following table briefly describes the tools.

Table 1.1 - Summary of the *ForeView* Tools

Tool	Description
Front Panel View	Provides a graphical representation of an actual FORE Systems’ ATM switch, including the number and type of network modules installed in the device, the status of the ports on each of these modules, and the Internet name for the Ethernet Port and Control Port. Also allows you to monitor network links and devices and provides a detailed view of a FORE Systems’ LAN-access devices such as PowerHubs, ES-3810s, and the CellPath products. See the *ForeView* Device Manager manual for information about the front panels for these devices.
AMI	Starts a telnet session to an ATM switch called up from Front Panel. By default, log in as “asx” to access the built-in administrative tools.
Graphing	Select one of four graphing options: switch ports, switch paths, switch channels, or hosts. This method works for graphing network usage for switches, links, and hosts in your network.
Logging	Select one of four logging options: switch ports, switch paths, switch channels, or hosts. This method works for logging network usage for switches, links, and hosts in your network.
Virtual Circuit Management	Select the Virtual Channel/Path tool for the creation of Paths (Through Paths, Signalling Paths), PVCs, and Smart PVCs. The tool allows users to create and modify VCs through a common interface.

Table 1.1 - Summary of the *ForeView* Tools

Tool	Description
Trace Paths/Channels	Traces VCs hop-by-hop through the network. Useful in troubleshooting by isolating connectivity problems.
Inventory	Allows network administrators to collect information about FORE ATM switches, edge devices, and host adapters. Useful for planning upgrade strategies, configuration profiles, and obtaining addresses.
Stand-alone Map	Starts an alternate map that can be run with the NMS or separately from the command line.
Call and Performance Records	Call and Performance Records are collection utilities for billing and maintenance purposes. Call Records collects information on a “call” basis at the VC and VP level, while Performance Records collects port activity information.
OAM Cell Monitor	FORE provides the OAM (Operations and Maintenance) utility to track switch traffic problems.
Upgrade Switch Software	FORE provides a switch software upgrade utility to download new and upgraded software, greatly simplifying and accelerating enterprise-wide software upgrades.
On-line Help	FORE provides on-line help in HTML format. FOr more information, see section 1.5 in this chapter.

1.3 Integration with Network Management Systems

ForeView is fully integrated with HP OpenView, NetView for AIX, and SunNet Manager network management systems. *ForeView* offers powerful graphic utilities for displaying chassis, interface, and port status information of a FORE ATM network that can be launched from network topology windows. *ForeView* uses many of these graphic views to display status information by switch and port using color and legend indicators. The integration of *ForeView* with these network management systems provides an intuitive, graphical set of applications that aid the network administrator in creating, modifying, and monitoring ATM networks.

1.3.1 HP OpenView and NetView for AIX

HP OpenView provides a management application called Network Node Manager (NNM) for use in managing TCP/IP networks and network devices that support SNMP. This application runs under the HP OpenView Windows (OVW) graphical user interface. HP OpenView provides configuration, performance, and fault management support for multi-vendor networks.

HP OpenView provides topology maps based on the discovered ATM information. The maps provide a graphical and hierarchical representation of the ATM network. When *ForeView* is integrated with HP OpenView and NetView for AIX, a *ForeView*-specific menu pull-down is added to the OpenView/NetView menu bar, as illustrated in Figure 1.1. Please refer to Chapter 5 for information on how *ForeView* works with HP OpenView and NetView for AIX.

1.3.1.1 A Note About NetView for AIX

NetView for AIX is developed by IBM, which purchased the source code for HP OpenView from Hewlett Packard and then began a separate development path. However, there are many similarities between the two platforms. For example, NetView processes have names that start with “ov”. Because the two platforms are very similar, we have combined information about OpenView and NetView into one chapter using examples based on OpenView.

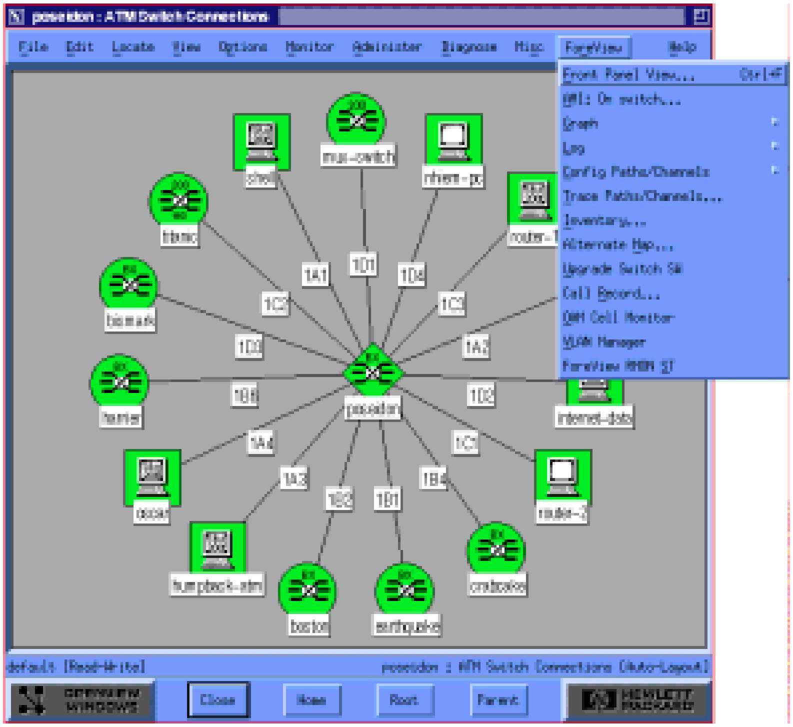


Figure 1.1 - HP OpenView with Integrated *ForeView*

1.3.2 SunNet Manager

SunNet Manager provides a comprehensive set of tools and services that can be used to perform fundamental network management tasks. SunNet Manager provides both management applications and agent software. The applications are processes that initiate management tasks and collect information. The agents are processes that access a device or element being managed at the request of an application. The SunNet Manager platform also supports customized network management applications such as *ForeView*.

The SunNet Manager console is the central management application of the system. When *ForeView* is integrated with SunNet Manager, the *ForeView*-specific applications are consolidated into the pull-down **`Tools`** menu within the SunNet Manager Console, as illustrated in Figure 1.2. Please refer to Chapter 6 for information on how *ForeView* works with SunNet Manager.

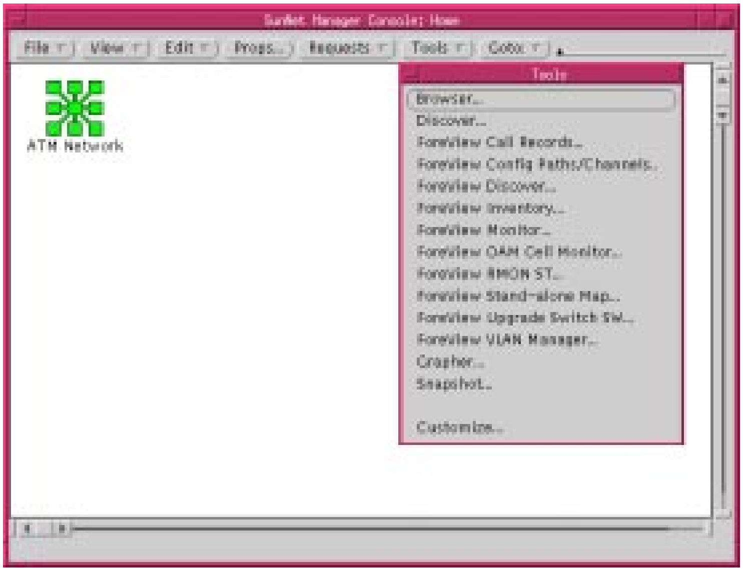


Figure 1.2 - SunNet Manager Console with Integrated *ForeView*

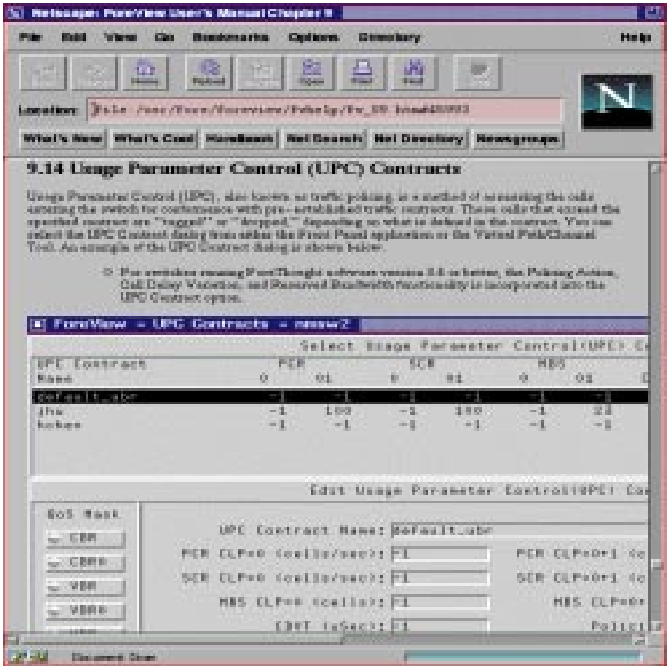
1.4 Discovery and Topology Mapping

ForeView provides applications for discovering and mapping ATM networks to provide a campus view of interconnected FORE switches and devices. Because ATM is connection-oriented, ForeView provides topology information representative of the physical network. Discovery is done via ATM signalling (UNI 3.x and/or SPANS). Any UNI 3.x or SPANS compliant device can be discovered, connection relationships can be determined, and the data can be displayed into specific map views.

A client/server architecture for discovery and status monitoring provides for scalability and true distributed network management. A network administrator can customize the discovery and status polling capabilities of *ForeView* to effectively manage networks with hundreds of switches. The discovery and status daemon serves the network topology information to any of the supported NMSs (HP OpenView, NetView, SunNet Manager) as well as the stand-alone *ForeView*. For more information on network discovery, refer to Chapter 4, Network Discovery.

1.5 On-line Help

ForeView provides an on-line Help manual in HTML format to assist you during network management tasks. You can get on-line help by clicking on the Help buttons found on the *ForeView* dialogs. A display similar to Figure 1.3 provides help related to the task you are performing.



9.14 Usage Parameter Control (UPC) Contracts

Usage Parameter Control (UPC), also known as traffic policing, is a method of [illegible] the cells entering the switch for conformance with pre-established traffic contracts. Those cells that exceed the specified contract are "tagged" or "dropped," depending on what is defined in the contract. You can select the UPC Contract dialog from either the Front Panel application or the Virtual Path/Channel Tool. An example of the UPC Contract dialog is shown below.

- For switches running ForeThought software version [illegible] or better, the Policing Action, Call Delay Variation, and Reserved Bandwidth functionality is incorporated into the UPC Contract option.

ForeView - UPC Contracts - [illegible]

Select Usage Parameter Control(UPC) C

UPC Contract	PCR		SCR		MBS	
Name	0	01	0	01	0	01
default_ubr	-1	-1	-1	-1	-1	-1
jhs	-1	100	-1	100	-1	22
[illegible]	-1	-1	-1	-1	-1	-1

Edit Usage Parameter Control(UPC) Co

QoS Mask
CBR
CBR0
VBR
VBR0

UPC Contract Name: default_ubr
PCR CLP=0 (cells/sec): -1
PCR CLP=0+1 (c
SCR CLP=0 (cells/sec): -1
SCR CLP=0+1 (c
MBS CLP=0 (cells): -1
MBS CLP=0+
CDVT (uSec): -1
Polici

Figure 1.3 - On-line Help Example

1.6 Automatic Error Tracking

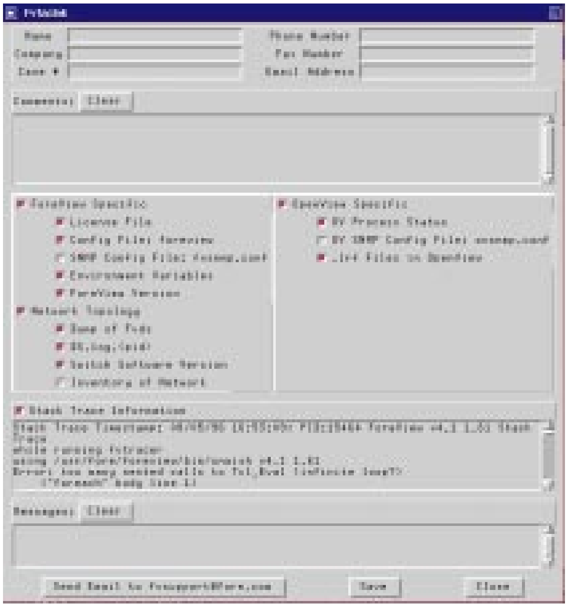
To aid FORE Systems' Technical Assistance Center (TAC) identify any problems you may encounter, a new mechanism called *ForeView* TACLink (fvtaclnk) has been implemented for reporting bugs to FORE Systems Technical Support.

Use TACLink to send information to FORE Systems' support group about an error or stack trace you may have encountered while using *ForeView*. If you specify a stack trace file name, the appropriate file is loaded in the display and is e-mailed to FORE Systems' technical support.

NOTE

If a stacktrace file is not specified, the **`error.log`** file in **`/usr/fore/foreview/tmp`** directory is sent (as long as the environment variable **`FOREVIEW_HOME`** is set).

Selectable filter options (*ForeView* Specific, Network Topology, OpenView Specific) provide additional information to aid in troubleshooting your problems. In addition, use the Comments box to provide additional configuration information (SNMP configuration, software version, etc.)



☒ ForeView Specific
☒ License File
☒ Config File: foreview
□ SNMP Config File: fvsnmp.conf
☒ Environment Variables
☒ ForeView Version
☒ Network Topology
☒ Dump of Fvdb
☒ SS,log,(pid)
☒ Switch Software Version
□ Inventory of Network
☒ OpenView Specific
☒ OV Process Status
□ OV SNMP Config File: ovsnmp.conf
☒ .lrf Files in OpenView
☒ Stack Trace Information

```
Stack Trace Timestamp: [illegible] PID:[illegible] ForeView v4.1 1.61 Stack
Trace
while running fvtracer
using /usr/fore/foreview/bin/fvwish v4.1 1.61
Error: too many nested calls to Tcl_Eval (infinite loop?)
    ("foreach" body line 1)
```

Figure 1.4 - *ForeView* TACLink Dialog

1.7 Unpacking Information

Upon receipt of, and before opening, your *ForeView* Network Management software, inspect the package for any damage that may have occurred during shipping. If the package shows any signs of external damage or rough handling, notify your carrier's representative.

When unpacking the *ForeView* Network Management software be sure to keep all original packing materials. They may be needed for return of the product.

CAUTION ⚠

All products returned to FORE Systems, under warranty, must be packed in their original packing materials.

1.8 System Requirements

Before installing *ForeView* network management software, be sure you have a platform which meets the following requirements. You will need to have the root password for the machine on which you wish to install *ForeView*.

1.8.1 Hardware

System: Sun

- SPARCstation (SPARCstation 10 Recommended)
- Ethernet, ATM SBA-200, or SBA-100 Network Interface (SBA-200 Recommended)
- Color monitor
- Free Disk Space: 32MB (minimum)
- Swap Space (Stand-alone): 64MB (minimum)
- Swap Space (OV, SNM): 96MB (minimum), 128 (recommended)
- Memory: 32MB (minimum) (64 MB recommended)

System: HP

- HP9000, Series 700
- Ethernet or ATM HPA-200 Network Interface
- Color monitor
- Free Disk Space: 32MB (minimum)
- Swap Space (Stand-alone): 64MB (minimum)
- Swap Space (OV, SNM): 96MB (minimum), 128 (recommended)
- Memory: 32MB (minimum) (64 MB recommended)

System: PC

- IBM-compatible PC with a Pentium CPU
- Ethernet or ATM ESA-200PC Network Interface
- Color monitor (1024 x 768, 256 colors)
- Free Disk Space: 100MB (minimum)
- Memory: 64MB (minimum)
- Mouse required, Microsoft or Logitech compatible

System: SGI

- MIPS R4000 series machines
- Ethernet or ATM GIA-200 Network Interface
- Color monitor
- Free Disk Space: 32MB (minimum)
- Swap Space (stand-alone): 64MB (minimum)
- Memory: 64MB (minimum)

System: AIX

- RISC System / 6000 POWERstation or POWERserver
- Ethernet or ATM Network Interface
- Color monitor
- Free Disk Space: 130MB (minimum)
- Swap Space (stand-alone): 64MB (minimum)
- Paging Space: 192 MB recommended
- Memory: 64MB (minimum)

1.8.2 Software

System: Sun

- Solaris 2.5.x
- HP OpenView SNMP Platform or NNM Version 4.11
- SunNet Manager 2.2.2
- Netscape Navigator 3.0

System: HP

- HP-UX 10.10 or 10.20
- HP OpenView SNMP Platform or NNM Version 4.11
- Netscape Navigator 3.0

System: PC

- Microsoft Windows NT 4.0

NOTE

The user's file system must support long file names.

- Netscape Navigator 3.0 or Microsoft Internet Explorer (MSIE) 3.0 or 4.0 (NOTE: See Release Notes for information regarding MSIE performance running under Windows NT.)

System: SGI

- IRIX 5.3, 6.2
- Netscape Navigator 3.0

System: IBM

- AIX 4.1
- NetView 4.x
- Netscape Navigator 3.0

CHAPTER 2 Software Installation

This section is designed to guide you through the installation of the *ForeView* Network Management software onto your system. The procedures contain step-by-step instructions for the successful installation of the software along with start-up and registration information. It is strongly suggested that you read all of this information carefully before attempting installation.

NOTE

ForeView should be installed AFTER HP OpenView or SunNet Manager is installed.

NOTE

For Unix users, if you are re-installing the *ForeView* software over an earlier version, please perform the re-installation procedure that follows. If this is a new installation, follow the installation instructions for the platform you are using.

NOTE

For VLAN Manager users, save your existing configuration to a local file before installing the new VLAN Manager from the *ForeView* CD-ROM. See “Creating a Local Backup File” in Appendix A of the VLAN Manager User’s Manual for information on saving a local file.

2.1 Obtaining the Software Distribution

Before beginning the installation process, you will need the software distribution from FORE Systems. This file can be obtained via FTP or CD-ROM. To obtain the file via FTP, you must have FTP access. To obtain the file from CD-ROM, you will need the distribution CD-ROM from FORE Systems.

You will also need a UNIX workstation with at least 32 Mbytes of free disk space. If you are installing from the CD-ROM, the UNIX workstation must also be equipped with a CD-ROM drive.

2.1.1 Obtaining the Software Distribution via FTP

The software can be retrieved from FORE Systems via anonymous FTP using the following procedure. First, FTP to `ftp.fore.com`. and log in as `anonymous`. Enter your full e-mail address (e.g., `jdoe@somewhere.com`) when you are prompted for a password.

NOTE

For security reasons, your password is not echoed.

Once you connect to FORE's FTP site (you will see the `ftp>` prompt), you must change to the `/priv/release/sunny` directory. This directory contains the *ForeView* software distribution files as well any .readme files which may contain important information about the software release.

NOTE

Because the contents of this directory cannot be listed, please contact FORE Technical Support to obtain the latest list of file names.

Any .readme files can be retrieved as ASCII text. However, before you retrieve the software files, you must switch the transfer mode to `binary`.

The following script is an example of how you might retrieve the software and .readme files. User input is shown in **`bold courier`** font.

```
server-jdoe:52=> ftp ftp.fore.com
Connected to ftp.fore.com.
220 ftp.fore.com FTP server (Version wu-2.4(4) Tue Apr 11 13:53:34 EDT 1995) ready.
Name (ftp.fore.com:jdoe): anonymous
331 Guest login ok, send your complete e-mail address as password.
Password:  TYPE YOUR FULL E-MAIL ADDRESS HERE <ENTER>
230-
230-               WELCOME to the FORE Systems FTP Server!
230-
230-  We are currently making many changes to the server to make it easier
230-  for you use and search for the files that you are looking for.
230-  Announcements regarding these changes will be posted here as they
230-  are completed.
230-
230-  If you have any problems finding the files that you are looking for,
230-  you can contact FORE Systems Technical Support by phone or send email
230-  to support@fore.com.
230-
230-  Abuse of any FORE Systems Technical Services system is grounds for the
230-  immediate removal of all access.
230-
230-
230 Guest login ok, access restrictions apply.
ftp> cd /priv/release/sunny <ENTER>
250 CWD command successful.
ftp> get fv43.readme <ENTER>
200 PORT command successful.
150 Opening ASCII mode data connection for fv43.readme (51578 bytes).
226 Transfer complete.
local: fv43.readme remote: fv43.readme
51578 bytes received in 1 seconds (50 Kbytes/s)
ftp> binary <ENTER>
200 Type set to I.
ftp> get fv43_hpux.tar.Z <ENTER>
200 PORT command successful.
150 Opening BINARY mode data connection for fv43_hpux.tar.Z (8147013 bytes).
226 Transfer complete.
local: fv43_hpux.tar.Z remote: fv43_hpux.tar.Z
8147013 bytes received in 2.3e+02 seconds (35 Kbytes/s)
ftp> quit <ENTER>
221 Goodbye.
```

2.2 Re-installation Procedure

If you are running on a Unix platform and have an older version of *ForeView* software, you will have to remove the older version prior to installing this version.

1. Exit all *ForeView* applications.
2. Exit your network management system (HP OpenView, NetView, or SunNet Manager).
3. If *ForeView* is installed in an alternate directory, make sure that the environment variable **`FOREVIEW_HOME`** is set.

NOTE

If *ForeView* is installed in an alternate directory it is imperative that you set the **`FOREVIEW_HOME`** environment variable before you begin the removal to avoid problems during the procedure.

4. Log in as root.
5. We recommend that you save your existing configuration and license files. To do this, issue the following commands:

```
cp /usr/fore/foreview/conf /tmp/foreview

cp /usr/fore/foreview/license /tmp/fvlicense
```

6. Issue the following commands:

```
/bin/sh /usr/fore/foreview/install/remove.sh

rm -rf /usr/fore/foreview
```

You are now ready to install the latest version of *ForeView*. The software installation instructions have been divided into two sections, installation procedures for Unix platforms and for the Windows NT Stand-alone platform. Please proceed to the installation instructions for the platform you are using.

NOTE

All users of *ForeView* on the OpenView platform must be informed that their personal configuration file **($HOME/ .foreview**) needs to be updated to reflect any changes in the system-wide configuration file (**$FOREVIEW_HOME/conf/foreview**).

2.3 Before You Begin

Before you begin the *ForeView* installation, make sure you have the following information:

- Your *ForeView* distribution, either via FTP or CD-ROM with installation instructions, and
- Your permanent *ForeView* license key.

NOTE

For larger ATM networks (200+ switch fabrics), the *ForeView* discovery and status daemon (**`fvdsd`**) can be run on multiple machines, thus partitioning the ATM network and distributing the SNMP load over several machines. If you would like to use this feature, please refer to Section 2.3.2 that follows for the installation requirements. Also, refer to Scaling Network Discovery in Chapter 4 for more information.

2.3.1 Software License Key

ForeView checks to see if you have a license file in **`/tmp/fvlicense`** OR in **`/usr/fore/foreview/conf/license`**. If a license file is not found, *ForeView* asks you to enter the license information, or it generates a 15 day temporary license.

To receive a permanent license key, please fill in all the information on the License Certificate and fax the card to FORE Systems' Technical Support.

2.3.2 Installation Requirements for Partitioning the Network

To run multiple daemons to distribute SNMP load on multiple machines, you need to list the machines you want to run the daemons on, and for each daemon, you need to list ALL the switches that the daemon is supposed to monitor. During the installation, you will be promted to list the machines where the daemons will run. The specification for each daemon has the following format:

```
<host_name>:<port>
```

where host_name is the name of the host where a daemon will be running, and the port (usually 7890). An example is:

```
nmsw1:7890, nmsw2:7890, nmsw3:7890
```

2.4 Installation from FTP File

If you have retrieved a software file with a .Z extension, then you need to uncompress the file using the following command:

```
uncompress <filename>
```

where *<filename>* represents the full name of the software file you have retrieved. For example, using the software file from the previous example:

```
uncompress fv43_hpux.tar.Z
```

NOTE After the software distribution is uncompressed, do NOT untar the file. The **install** procedure will expect the software distribution to be in tarfile format.

NOTE There are separate distribution files for UNIX platforms. For example, fv43_hpux.tar.Z for HP, and fv43_sol.tar.Z for Solaris.

2.4.1 Software Installation

1. To install *ForeView* software after uncompressing the tar file, change to the `/usr/fore` directory by entering **`cd /usr/fore`**.
2. Extract the installation script by entering **`tar -xvf fv43_hpux.tar`**.
3. Run the following command to begin installation: **`./install.sh`**.
4. Answer the questions that follow to complete the installation.

NOTE If you wish to install foreview in an alternate location (other than **`/usr/fore`**), please follow the instructions in Section 2.5.2.

2.5 Installation from CD-ROM

The install program automatically determines the platform and the operating systems that you are using. If the management platform is not installed in the default locations, *ForeView* will ask you to enter the location. Also, you will be asked for confirmation on the platform.

NOTE

If you wish to install foreview in an alternate location (other than **`/usr/fore`**), please follow the instructions in section 2.3.2.

2.5.1 UNIX Platform

1. Insert the *ForeView* Network Management x.x CD-ROM into the CD-ROM drive and mount the file system as **`/cdrom`**. See your system's user guide for instructions on mounting CD-ROMs.
2. Change directory to **`/cdrom/unix`**.
3. Run the following command to begin the installation:
   ```
   ./install.
   ```
4. Answer the questions that follow to complete the installation.

2.5.2 Software Installation in an Alternate Directory

It is strongly recommended that you install foreview under **`/usr/fore`**. If you do not have enough disk space under **`/usr`**, you can create a link to a file system that does have enough space (**`your_alternate_fs`**, for example):

```
cd /usr

ln -s your_alternate_fs /usr/fore
```

Then, follow the instructions described in 2.3.1.

If you do not want to install under **`/usr/fore`** <u>and</u> you do not want to create a link to another file system, you can install *ForeView* in an alternate directory (**`/usr/local`**, for example).

Make sure you (and every *ForeView* user on your system) set the environment variable **FOREVIEW_HOME** to **/usr/local/foreview**. Also do that in the appropriate login shell startup file (.profile, .cshrc, .kshrc, etc.). The example below assumes you are running csh.

1. Enter the following commands:

   ```
   setenv FOREVIEW_HOME /usr/local/foreview

   cd /usr/local (instead of /usr/fore)
   ```

2. Follow the installation instructions described in 2.3.1.

NOTE

If you forget to set the environment variable **FOREVIEW_HOME** before you start the install into a directory other than **/usr/fore**, you may see errors like the following during customization.

If running under HP OpenView:

```
object manager name: fvovtrapd
behavior:            OVs_WELL_BEHAVED
state:               FAILED
PID:                 11009
last message: could not open license file /usr/fore/foreview/conf/license
exit status:         -
object manager name: fvovmon
behavior:            OVs_WELL_BEHAVED
state:               FAILED
PID:                 11010
last message:        could not open license file /usr/fore/foreview/conf/license
exit status:         -
WARNING: Some daemons did not successfully restart:
WARNING: fvovmon did not successfully initialize.
WARNING: You will have to start it using ovstart.
WARNING: fvovtrapd did not successfully initialize.
WARNING: You will have to start it using ovstart.
```

In that case, please set the environment variable as mentioned above, do a ovstop and ovstart:

```
setenv FOREVIEW_HOME /usr/local/foreview

/usr/ov/bin/ovstop

/usr/ov/bin/ovstart
```

If running under SunNet Manager:

You may see a message on **stderr** when you select **Discover** from the *ForeView* Discover application:

```
fvsnmdsc cannot find application files
```

In this case, exit SunNet Manager, set the environment variable as mentioned previously and restart snm:

```
setenv FOREVIEW_HOME /usr/local/foreview

snm -i
```

If running Stand-alone:

Set the environment variable as mentioned previously and run the application again.

2.5.3 Windows NT Installation

The following software installation and configuration instructions have been prepared for the Windows NT platform.

NOTE

A mouse is required to run *ForeView* on a PC running Windows NT.

1. Insert the *ForeView* Network Management x.x CD-ROM into the CD-ROM drive.
2. From the File Manager, select the CD-ROM drive.
3. From the File Manager, select the **Windows** directory on the CD-ROM.
4. Select **Setup.exe** from the list of files in the File Manager.
5. Pull down the File menu from the File Manager and select **Run**.
6. Continue with the installation by following the screen prompts.

NOTE

You must turn OFF the Full Drag option under **Control Panel\Desktop** to optimize screen refresh capabilities.

7. Edit the ForeView configuration file, **foreview\conf\foreview.conf**, described in more detail in Chapter 3.

After you have completed the installation and configuration of *ForeView*, you may want to turn to Chapter 7, “Running *ForeView’s* Stand-alone Map”.

2.5.4 Import the Host Name File

When running *ForeView* on Windows NT, the file **hosts** must be imported to have all the host names available. To import this file, do the following:

On a UNIX workstation:

1. Enter the following command:

```
ypcat hosts > hosts
```

2. Copy this file, via ftp, to the drivers directory on your local machine, such as:

```
\winnt35\system32\drivers\etc
```

If you have a UNIX partition on your local machine:

1. Start the network from the control panel.
2. Configure TCP/IP.
3. Select **Advanced** in the TCP/IP Configuration dialog.
4. Check **Enable LMHOSTS** lookup.
5. Click on **Import LMHOST**S.
6. Enter the directory path where the file is located and select **Import**.

NOTE

The file LMHOSTS is copied to your **\winnt35\system32\drivers\etc** directory.

7. Rename the file **LMHOSTS** to **HOSTS**.

CHAPTER 3 Configuring *ForeView*

ForeView includes a configuration file template to edit after the software is installed. This configuration file contains resources that apply to *ForeView* running under a network management system (such as HP OpenView, NetView for AIX, or SunNet Manager) and the Standalone Map version. This chapter covers the basics of *ForeView* configuration.

3.1 Overview

Applications running under *ForeView* look to the configuration file to find what values have been defined for certain resources. Specifically, editing the configuration file allows you to:

- Define a list of Fore ATM switches to be used by the discovery and status daemon (fvds daemon) as starting points for network discovery.
- Create customized Map Views based on multiple switch order/seed switch configurations.
- Specify graphing utility options for HP Openview platforms.
- Specify the maximum number of points to be displayed by **`fvbltgr`**.
- Enable the reserved channels display.
- Define status polling intervals.
- Define mappings that link clustered switches' names and enclosure identifiers with more recognizable names.
- Specify the SNMP configuration file location, either HP OpenView's file or *ForeView*'s file (see section 3.2).
- Provide for more precise configuration of *ForeView* by specifying the advanced configuration resources (see section 3.3).

For Unix users, the *ForeView* configuration file can be found in the following directory:

```
$HOME/.foreview
```

and in

```
$FOREVIEW_HOME/conf/foreview
```

The first file, **`$HOME/.foreview,`** is the “site-wide” configuration file. The second file, **`$FOREVIEW_HOME/conf/foreview`**, is the local user’s configuration file. Resources in the user’s configuration file always override those of the site-wide configuartion.

For PC users, the *ForeView* configuration file can be found in the following directory:

```
foreview\conf\foreview.conf
```

3.1.1 General Format

The general format of an entry in the *ForeView* configuration file is as follows:

```
ResourceName: value [, value] [, value] ...
      or
Specifier.ResourceName: value [, value] [, value] ...
```

That is, you can define a general resource or a specific resource and give that resource a comma-separated list value. The resources in the sample configuration file have not been defined. Instead, they are all commented out. To enable any of the resources, remove the comment marks and enter the appropriate value or values.

NOTE

The values found in the template are example values and are not guaranteed to be valid for your installation.

3.1.2 Discovery Server

ForeView utilizes a discovery and status server application that discovers *ForeRunner* switches, NNI and UNI links, and the endpoints of NNI and UNI links in an ATM network. This application, **`fvdsd`**, has two tasks. First, the application discovers the network elements and polls the information to keep its own internal cache up-to-date. Second, it makes the network topology and status information available to clients through a TCP socket.

All switches and devices connected to any of the switches in the list, which can be communicated with via IP and/or SNMP, will be discovered and monitored, by default.

For example:

Fvds.discSwitches: switch1, switch2

In this case, the discovery process will discover “switch1” and “switch2” and all of the two switches’ direct and indirect ATM neighbors.

NOTE

This resource defines the switches that the daemon **fvdsd** uses to discover the rest of the network, and does NOT specify what the applications will use to show on a map.

3.1.3 Alternate Discovery

The use of **SwitchOrder** and **SeedSwitches** is a way to restrict the list of switches retrieved from **fvdsd**. These resources do not initiate network discovery. In general, most users would not use them.

The seed switches are provided in the configuration file using two entries. First, you must designate a list of switches, called a **SwitchOrder**. The discovery process will discover each switch in the **SwitchOrder**. The order of the list may be important for Stand-alone map **(fvmap)** users who want to display the discovered switches in a particular order.

Second, switches may be designated as seed switches by including them in the **SeedSwitches** entry. The discovery process uses each seed switch to find ATM neighbors to add to the database.

In the simplest case, the **SwitchOrder** entry and the **SeedSwitches** entry each contain the name of one switch in the ATM network. For example:

```
SwitchOrder:      angler
SeedSwitches:     angler
```

In this case, the application process will retrieve from the **fvdsd** “angler” and all of angler’s direct and indirect ATM neighbors.

NOTE

For each ATM "cloud" (set of connected ATM devices), only 1 switch in each cloud needs to be included in the lists.

3.1.4 Stand-alone Map Display Order

The *ForeView* Stand-alone Map has a **`View`** option that determines the layout of the map. The following options are available:

default Shows the complete ATM network layout based on the switch order / seed switch entry.

mapViews Allows user-configurable map layouts, based on specific switch order / seed switch combinations.

By defining a subsequent switch order for each **`mapView`**, you can partition the network into ATM "subnetworks". You can also define a subsequent seed switch list for each **`mapView`**. For example:

```
Fvmap.mapViews: accounting, engineering

accounting.switchOrder: switch1, switch2

accounting.seedSwitches: switch2

engineering.switchOrder: switch3, switch4

engineering.seedSwitches: switch4
```

3.1.5 Stand-alone Map NNIs

The **`fvmap`** application will explode a switch to show only its neighbor switches (NNIs) when the value for **`Fvmap.NNIsOnly`** is set to **`TRUE`**. When **`FALSE`**, all the neighbors of a switch, including other switches and connected hosts, will be shown. For example:

```
Fvmap.NNIsOnly: TRUE
```

NOTE Valid for *ForeView* 4.0.x and earlier releases.

3.1.6 Graph Type

The resource **FvGrapher** defines which graphing application to use to graph statistics gathered from managed devices. By default, **fvbltgr** will be used for *ForeView*-SNM and *ForeView*-Stand-alone. For *ForeView* running under HP OpenView, the OpenView **xnmgraph** utility will be used. The only recognized values for this resource are **fvbltgr** and **xnmgraph**. For example:

```
FvGrapher: fvbltgr
```

NOTE

For more information on **fvbltgr** and **xnmgraph**, see the corresponding man pages **fvbltgr(1)** and **xnmgraph(1)**.

3.1.7 Maximum Points to Display

The resource **Fvbltgr.maxPoints** defines the maximum number of points that the graphing application **fvbltgr** can display. If left to run for an extended period of time, **fvbltgr** can consume significant resources. By setting the `maxPoints` resource, the amount of memory used by **fvbltgr** can be limited. The default value for **maxPoints** is 2000. You may enter another value to override the default. For example:

```
 Fvbltgr.maxPoints: 300
```

3.1.8 Displaying Reserved Channels

The **ShowReserved** resource takes a boolean value **TRUE** or **FALSE**. If **TRUE**, then the applications that provide lists of channels will include the reserved channels 15 and 16 in their lists. If **FALSE**, those channels will not be included. The default is **FALSE**. For example:

```
ShowReserved: TRUE
```

3.1.9 Status Polling

The resource **Fvmap.pollInterval** defines the polling interval for updating the status of switches and hosts that are being shown in the map in seconds. For example:

```
Fvmap.pollInterval: 30
```

3.1.10 Enclosure Identification Name Mapping

The *ForeRunner* ASX-1000 switch can contain a cluster (multiple switches) within a single enclosure. Each enclosure has a unique enclosure id number. When a switch within an enclosure is discovered by *ForeView* running under HP OpenView, SunNet Manager, or the Standalone map, the name given to the switch has the form: **`switchname(enclosure id)`**, and the name given to the entire enclosure would be **`enclosure <encl id>`**. Because the enclosure id numbers may not be particularly readable, a network manager can map an enclosure id number to a string. For example, if the enclosure id was 1434302, then the line:

```
ClusterName.1434302: Cluster1
```

would map 1434302 to the name "Cluster1", and a switch in this cluster would be labeled "switchname(Cluster1)".

3.2 Configuring SNMP

ForeView comes with a default SNMP configuration file used to retrieve SNMP configuration information. All *ForeView* applications read this file to retrieve custom SNMP configuration information. By default, *ForeView* uses the SNMP configuration information that comes from **`$HOME/.fvsnmp.conf`**; or, **`$FOREVIEW_HOME/conf/fvsnmp.conf`**.

3.2.1 Aligning SNMP Configuration with HP OpenView SNMP Configuration

Because HP OpenView already supports a customization file for SNMP configuration, users of HP OpenView also may wish to use that file for *ForeView* SNMP configuration. To use the HP OpenView SNMP file, uncomment the following line in the configuration file. For example:

```
FvsnmpConfFile: /usr/OV/conf/ovsnmp.conf
```

For OpenView 4.0 on Solaris (and HPUX10.x), users should set **`FvsnmpConfFile`** to point to **`/etc/opt/`**.

3.2.2 Community Names

The format for the SNMP configuration file is as follows:

```
target:rd-comm:proxy:timeout:retries:poll:port:wr-comm:
```

Valid options for each variable are:

target Source of SNMP queries. Valid options for this field are DNS name, IP address, and *.*.*.* wildcard entry in any combination.

rd-comm Read Community string. Default is “public”.

proxy Default is none.

timeout Default setting for timeout is 8 (tenths of seconds).

retries Default setting for retries is 3.

poll Not used.

port Default setting is standard SNMP port 161.

wr-comm Write Community string. Default is “private”.

3.3 Advanced Configuration

Several resources provide for more precise configuration of *ForeView*. Specifically, the advanced configuration resources allow the following:

- Host interface display configuration, which uses an algorithm to determine the properties of remote endpoints.
- Link status propagation, which allows a switch symbol on the “ATM Networks” submap to derive its status from underlying submap elements, including the links.
- Management status mode, which allows you to explicitly define the set of ports on switches that should be managed, and those that should be ignored.
- Distributed discovery setup.
- Recognizing and managing new FORE or non-FORE devices.

3.3.1 Host Interface Preferences Configuration

For each link that is discovered, the *ForeView* discovery server **fvds** tries to discover information about the remote endpoint of the link. However, because no physical link information is available via SNMP, **fvds** instead retrieves logical link (signalling path) information. Thus, for each port on a switch, **fvds** retrieves the sigpath information, including the remote endpoint of the sigpath.

As ATM Networks grow and diversify, the use of multiple signalling paths on a single port has become more common. When this happens, **fvds** discovers multiple logical links emanating from a single physical port. Because remote endpoint information is retrieved for each sigpath on a link, there is a need to summarize or combine this information to determine the properties of the host.

Currently, network topology information displays a single link to represent the physical link on a port and a single host to represent the remote endpoint of that link. Then, the sigpaths on that link are displayed in a submap of the link symbol. Remote endpoint information is retrieved for each sigpath on a link. Thus, one needs a way to combine or summarize the endpoint information to determine the properties of the host symbol.

The properties of the signalling path and the endpoint information that can be used in determining the properties of the host include:

- Signalling path status
- Endpoint status
- Signalling path protocol type
- Remote IP address
- Remote ATM/NSAP address
- Remote port BNP
- Remote host type

The properties that are shown in the host symbol are:

- Status
- Label (usually an IP address or equivalent DNS hostname)
- Type (usually representing the remote host type)

ForeView takes the information for each sigpath and endpoint pair and combines this information with user preference information to produce an information set that will be used to create a host symbol.

3.3.1.1 User Preferences

User preferences allow you to determine which sigpath information should be used when multiple sigpaths exist. The user preferences may be defined in the following ways:

- Which signalling protocol, UNI 3.x or SPANS, takes precedence
- Which VPI for sigpaths takes precedence
- Which endpoint addresses or groups of addresses takes precedence

Given a list of sigpath/endpoint information, and a set of user preferences, the algorithm for determining which single set of sigpath/endpoint information to use to identify the host is a follows. The algorithm is essentially a series of filters for choosing which sets of information to reject, until only a single candidate remains. Thus, if at any step only one set of information remains, the algorithm is complete.

1. If there exists sigpaths from multiple signalling protocols and the user has specified a preference for one of the signalling protocols, reject the others.
2. If there exists sigpaths on multiple VPIs and the user has specified a preference for one of the signalling protocols, reject the others.
3. If the user has given a list of preferred endpoint addresses, and there exist sigpaths with endpoint addresses that do not match the user's preferences, reject the others.

4. If there are both sigpaths with status up and sigpaths with other statuses, reject the non-up sigpaths.
5. If there are both sigpaths with valid remote endpoint IP addresses and non-valid IP addresses (255's or all 0's), reject the sigpaths with non-valid IP addresses.
6. If there are both sigpaths with endpoints that are reachable amd non-reachable, reject the sigpaths with non-reachable endpoints.
7. If there are both sigpaths with known host adapter types and unknown host adapter types, reject the latter.
8. If there still exist multiple sigpaths candidate sigpaths, and there exist sigpaths from different signalling protocols (UNI 3.x vs. SPANS), then reject the SPANS signalling paths.
9. If there still exist multiple candidate sigpaths, then choose the sigpath with the lowest numbered VPI.

3.3.1.2 Specifying User Preferences

To specify explicitly which sigpaths should be used to determine which host information is shown on the maps, edit the configuration file. As stated previously, the three preferences are: which signalling protocol to use, which VPI to use, and which range of endpoint IP addresses to use.

NOTE

If no preferences are specified then the default signalling to use is UNI 3.x, see step 8 of the algorithm above. Additionally, if no user preferences are given for the choice of VPI, then the algorithm chooses the lower numbered VPIs over higher numbered VPI, see step 9 of the algorithm above.

For example, to specify that SPANS sigpaths take precedence over UNI 3.x sigpaths, place the following in the configuration file:

```
PreferSigType: SPANS
```

3.3.2 Link Status Propagation

A model for computing a circle switch symbol's status provides for the propagation of the down condition of a UNI link or a host to the level 1 or level 2 symbols. This model is in addition to the current existing (default) model.

In the new model, a circle switch symbol on level 2 derives its status from a combination of the statuses of the symbols in its submap. Specifically, given a circle switch symbol "A", A's status is derived from the statuses of the diamond switch symbol in A's submap and all the links in A's submap (but not the statuses of the hosts in A's submap).

If the diamond switch symbol for "A" is not "Normal", then the A's circle switch symbol has the same status as its diamond switch symbol. Otherwise, if the diamond switch symbol for A is "Normal" then the status of the links from the diamond switch are combined to compute the status of the circle switch symbol.

The resource **`Fvovmap.LinkStatusProp:`** when set to **`TRUE`**, allows a switch symbol on the "ATM Networks" submap to derive its status from the status of the center diamond switch symbol in the switch's submap AND the status of the links from that center diamond switch symbol.

3.3.3 Port Management Status Configuration

The **`-UseMgmtStatus`** mode allows you to explicitly define the set of ports on switches that should be managed, and those that should be ignored. This can be useful when you want to manage ports for which no signalling exists and hardware carrier status should be monitored and displayed. (In the default mode, if no hardware carrier exists on a port, then no information about the port is recorded by **`fvds`**.)

In **`-UseMgmtStatus`** mode, **`fvdsd`** discovers a link for every port on every switch for which the MIB variable **`portManagementStatus`** is set to 1 (managed). For more information on -**`UseMgmtStatus`**, see Chapter 4 (Network Discovery).

3.3.4 Distributed Discovery

The *ForeView* discovery and status daemon (**`fvdsd`**) serves data to clients using a TCP connection. Thus, the server and clients can communicate over a TCP/IP network. To make this happen, do the following steps:

On the "Server" machine, where **`fvdsd`** will run:

1. Install ForeView x.x, choosing the **SA** option during installation.
2. Edit the **`/usr/fore/foreview/conf/foreview`** file, specifying the server machine in the "Fvds.hostname" resource, and the TCP port in the "Fvds.port" resource (if you choose a port other than the default 7890).

3. Edit the **/usr/fore/foreview/conf/fvsnmp.conf** file if necessary, specifying the SNMP configuration needed.
4. Start up **fvdsd** by typing “fvds”.

On the “Client” machine, where OV, SNM, or the Stand-alone map (fvmap) will run:

1. Install ForeView x.x.
2. If not using OpenView, skip to step 4.
3. If using OpenView, as root, do “ovstop -v” to stop all daemons. (The installation script will have started up fvds on the local machine and the ForeView-OpenView daemons fvovmon and fvovtrapd will be using that server initially.) Then, do “ovdelobj /usr/OV/lrf/fvds.lrf”, so that subsequent “ovstart” calls will not start up a local ‘fvdsd’.
4. Edit the **/usr/fore/foreview/conf/foreview** file, specifying the server machine in the “Fvds.hostname” resource, and the TCP port in the “Fvds.port” resource (if you choose a port other than the default 7890).
5. If using OpenView, as root, do “ovstart -v” to restart all the daemons.

NOTE

A single instance of ’fvdsd’ can be used with multiple clients. For example, multiple copies of *ForeView* for OpenView could all use a single ‘fvdsd’ as their source of network topology and status.

3.3.5 Adding New Devices

Users can program *ForeView* to dynamically recognize and manage new FORE or non-FORE devices from within *ForeView*, at various levels of complexity. The resource **FvAccess** takes information you provide via the *ForeView* configuration file. This information is used by the *ForeView* for OpenView (FV-OV) daemons, the *ForeView* for SunNet Manager (FV-SNM) daemons, the *ForeView* Stand-alone (FV-SA) daemon, as well as the *ForeView* front panel application (fvpanel).

You can instruct *ForeView* that a device with a certain SNMP System Object Identifier is to be represented by a certain bitmap, icon, or glyph, and can be managed by launching a certain application. Alternatively, you can also specify the device type or IP address by providing the FORE switch and port to which the device is connected in the network.

3.3.5.1 How to use the FvAccess Mechanism

In order for a new device to be recognized, you must provide a unique identifier for the device type in the configuration file. The entry in the configuration file should be in the following format:

```
FvAccessDevices: <unique-device-id>
```

For example, suppose we choose to call this device identifier “AVA”. The entry would have the following format:

```
FvAccessDevices: AVA
```

NOTE

Multiple device types are provided in a comma-separated list, such as AVA, AVB, AVC.

By correctly editing the appropriate resources in the *ForeView* configuration file template, you can instruct **FvAccess** to do the following:

- To recognize a device type by its System Object ID by providing a binding in the format <unique-device-id>.sysOid: <system-object-id>.
- To instruct *ForeView* which application to launch to manage a device by providing a line which contains the name of the executable to launch in the form of <unique-device-id>.frontPanelApp: <executable-file-name>.
- To instruct *ForeView* on which icon/bitmap/glyph to use to represent the new device type by providing a line in the format <unique-device-id>.iconName: <iconname>.

3.3.5.2 Handling Non-IP, ATM-connected Devices

This feature is generally used when a device connected to a FORE switch does not communicate using IP or SNMP, preventing the device type from being specified using the SNMP system object ID. Instead, you instruct *ForeView* that a device connected to a switch's port corresponds to a certain device id. This information is provided in the following format:

```
<switch-name-or-ipaddress>/<port-number>.deviceType: <device-id>
```

For example,

```
switch1/1A1.deviceType: AVA
```

Again, because the device does not speak IP, *ForeView* cannot learn the IP address of the device to derive a hostname for the device. To instruct *ForeView* how to label the device, provide information in the following format:

```
<switch-name-or-ipaddress>/<port-number>.mapLabel: “some label”
```

For example,

```
switch1/1A1.mapLabel: My New Device
```

The result is that on the OpenView, SunNet Manager, Stand-alone maps, and on the front panel for the connected switch, the device should be labeled “My New Device”.

NOTE

This device type and device name will be used ONLY if *ForeView* cannot communicate with the device via IP. If *ForeView* can communicate with it via IP, then *ForeView* will use the IP hostname and device type that it can derive by communicating with the device itself.

3.3.5.3 Learning IP Addresses of Connected Devices

You can specify the IP address of an ATM-connected device when the IP address is not communicated correctly to a switch. This is useful when a device speaks IP, but does not signal its IP address correctly to its connected switch. Using this feature, you can tell the *ForeView* discovery and status daemon the IP address of the connected device, allowing the device to be shown correctly by the discovery and status daemon (OpenView, SunNet Manager, Stand-alone, etc.). To use this feature, provide information in the following format:

```
<switch-name-or-ipaddress>/<port-number>.ipAddress: <ipaddress>
```

For example,

```
switch1/1A1.ipAddress: 169.144.77.33
```

3.3.5.4 Additional Installation Instructions

This section outlines the additional steps required to make the **FvAccess** feature of *ForeView* work with the various configurations of *ForeView,* as well as applications within *ForeView.*

3.3.5.4.1 Front Panel

The front panel launcher reads the **FvAccess** specifications and uses the unique device id, sysOid, and frontPanelApp specifications to bind devices to executables. For example, enter the following:

```
fvpanel my-new-device
```

and get a front panel application activated against your machine named “my-new-device”.

3.3.5.4.2 Stand-alone Map

The stand-alone version of *ForeView* loads in all the **`FvAccess`** specification lines listed above. If **`fvmap`** finds a device connected to an ATM switch that has a sysOid that matches one given in the configuration file, **`fvmap`** retrieves a graphic file specified by the iconName binding and uses that graphic to represent the device. To use this to function, you need to provide six graphic files for the device and put them in a location where **`fvmap`** can find them.

The directory is **`$FOREVIEW_HOME/fvmap/gifs`**, which is typically bound to **`/usr/fore/foreview/fvmap/gifs`**. The filename has the following format:

`<iconName><color><size>.gif`

where

<color> is one of

"g" -- a gif with a green background to signify an "up" device.

"r"-- a gif with a red background to signify a "down" device.

"y"-- a gif with a yellow background to signify a "marginal" device.

and

<size> is one of

"3"-- a gif of size 64x32 pixels.

"5"-- a gif of size 100x50 pixels.

Additionally, providing this information allows you to successfully select the device in **`fvmap`**'s window and launch the front panel application against it successfully.

3.3.5.4.3 SunNet Manager Discovery

As with **`fvmap`**, the FV-SNM application, **`fvsnmdsc`**, loads in all the **`FvAccess`** specification lines listed above. If **`fvsnmdsc`** finds a device connected to an ATM switch that has a sysOid that matches one given in the configuration file, **`fvsnmdsc`** retrieves an "icon" file specified by the iconName binding and uses that glyph to represent the device. To get this to function, you must provide a ".icon" and ".iconmask" file for the device and put them in a location where **`fvsnmdsc`** can find them. The directory is **`/usr/snm/foreview/icons`** (or **`/opt/SUNWconn/snm/foreview/icons`**). The filename is the iconName specification given in the config file, with ".icon" (".iconmask") appended. For example, ava.icon and ava.iconmask.

To be able to launch the front panel application against the new device, one must provide information as in 6.1. above, and one must edit the foreview.schema file found in /usr/snm/struct/foreview.schema (/opt/SUNWconn/snm/struct/foreview.schema). Within this file, add a component record exactly the same as the “component.atm-host” record, with the name “component.<iconname>”, which <iconname> was given in the configuration file. Then, in the “instance elementCommand” record, add lines to allow one to launch applications for this new component type.

Finally, add a line to the “instance elementGlyph” record to bind the new component name to the icon name. Note that after you have edited these files, you MUST restart snm with the “-i” flag.

3.3.5.5 FV-OV Processes

As with **`fvmap`**, the FV-OV application processes, **`fvovmon`**, **`fvovtrapd`**, and **`fvovmap`**, load in all the **`FvAccess`** specification lines listed above. If the FV-OV processes find a device connected to an ATM switch that has a sysOid that matches one given in the configuration file, **`fvov`*** retrieves a symbol specified by the iconName binding and uses that symbol to represent the device.

You must edit the **`/usr/OV/symbols/C/Atmnet`** (**`/etc/opt/OV/share/symbols/C/Atmnet`**) file and add a record for the new symbol. The record should be similar to the following:

```
SymbolType “FV-Connector”: “<iconname>”

{

Filebase “<iconname>”;

CursorSize 38;

}
```

where <iconname> is the same as was specified in the *ForeView* configuration file. Next, you must make bitmap files for this symbol and place these files in the **`/usr/OV/bitmaps/C`** (**`/etc/opt/OV/share/bitmaps/C/foreview`**) directory, with the filenames <iconname>.<number>.{m,p}, where <number> is 20, 26, 32, 38, 44, and 50 (thus, 12 bitmap files have to be created and added to this directory). After performing these steps, you must restart OpenView by typing ovw.

The new device should sow up on the ATM Networks submap with the symbol type that you defined and the symbols that you provided. Additionally, you should be able to select the device and launch the front panel application from the *ForeView* menubar.

NOTE

On the IP map submaps, the device will not be shown with the correct device type. To fix this, edit OV's oid_to_type and oid_to_sym files in **/usr/OV/conf** (**/etc/opt/OV/share/conf**) and **/usr/OV/conf/C** (**/etc/opt/OV/share/conf/C**), respectively. Explanations for how to edit these files can be found in the file comments.

3.4 Configuration Template

```
# Template .foreview file.
#
# @(#)$Id: template,v 1.56 1997/03/20 20:28:19 schandra Exp $ FSI
#
# Copyright FORE Systems, Inc. 1995
#
# Version 4.1
#
# General format:
#      ResourceName: value [, value] [, value] ...
#              or
#      Specifier.ResourceName: value [, value] [, value] ...
#
# The resources each application looks to retrieve values for are listed
# in Chapter 3 of the ForeView 4.1 User Manual.
#
# All resources used in ForeView are discussed here.  No resources
# have been defined: they are all commented out.  All values given are
# only example values: they are not guaranteed to be valid for your
# installation.
#
# SwitchOrder: defines a list of Fore ATM switches to be shown in various
# applications.  Order of the list may be important for fvmap users.
#
# Applications that retrieve this resource: fvsnmdscd, fvmap, fvinv.
#
# SwitchOrder: switch1
# SeedSwitches: defines a list of Fore ATM switches to be used as seeds for
# finding neighbor switches during retrieval from fvdsd.  Order of this list
# does not matter.  All switches given in the list should be in the
# SwitchOrder list.  For each ATM "cloud" (set of connected ATM switches),
# only 1 switch in each cloud needs to be included in the list.  Note that
# this resource does NOT define what the daemon fvdsd will discover, but
# defines what the applications will get from the daemon.  To specify the
# switches that fvdsd uses to discover the rest of the network, use the
# resource Fvds.discSwitches below.
#
# Applications that retrieve this resource: fvsnmdscd, fvmap, fvinv.
#
# SeedSwitches: switch1
# Fvds.discSwitches: defines a list of Fore ATM switches to be used
# by the discovery and status daemon (fvds daemon) as starting points for
# network discovery.  All switches and devices connected to any of the switches
# in the list, which can be communicated with via IP and/or SNMP, will be
# discovered and monitored, by default.  Note that this resource defines
# the switches that the daemon fvdsd uses to discover the rest of the network,
# and does NOT specify what the applications will use to show on a map.
#
# Applications that retrieve this resource: fvdsd.
#
# Fvds.discSwitches: switch1, switch2
# FvsnmpConfFile: overrides which file is to be used to retrieve SNMP
# configuration information.  By default, it is the SNMP conf information
# that comes from $HOME/.fvsnmp.conf, or, $FOREVIEW_HOME/conf/fvsnmp.conf.
# ForeView-OV users may wish to uncomment out the following line so
# that the ovsnmp.conf used by HP OVW is also used for ForeView.
#
# Applications that retrieve this resource: all.
#
# FvsnmpConfFile: /usr/OV/conf/ovsnmp.conf
# FvGrapher: defines which graphing application to use to graph statistics
# gathered from managed devices.  By default, 'fvbltgr' will be used for
# ForeView-SNM and ForeView-StandAlone, and 'xnmgraph' will be used for
# ForeView-OV.  'fvbltgr' and 'xnmgraph' are the only recognized values.
#
# Applications that retrieve this resource: fvgraph*, fvtracer, fvasx, fvlax.
#
# FvGrapher: fvbltgr
# Fvbltgr.maxPoints: defines the maximum number of points that fvbltgr will
# plot before it starts to drop the oldest points.  By default, fvbltgr will
# show up to 2000 points.
#
# Applications that retrieve this resource: fvbltgr.
#
# Fvbltgr.maxPoints: 300
# Fvmap.mapViews: defines a list of views onto the ATM network.  By defining
# a subsequent switchOrder for each mapView, one can partition the network
# into ATM "subnetworks".  One can also define a subsequent seedSwitches list
# for each mapView.
#
# Applications that retrieve this resource: fvmap.
#
# Fvmap.mapViews: accounting, engineering
# accounting.switchOrder: switch1, switch2
# accounting.seedSwitches: switch2
# engineering.switchOrder: switch3, switch4
# engineering.seedSwitches:
# ClusterName.<enc_id>: defines a mapping between a cluster's (BXE's)
# enclosure identifier and a more human-readable name.
#
# Applications that retrieve this resource: fv-ov, fv-snm, fvmap, fvinv.
#
# ClusterName.123456789: MyFirstBXE
# Fvmap.NNIsOnly: this resource takes a boolean value 'TRUE' or 'FALSE'.  If
# TRUE, then fvmap will explode a switch to show only its neighbor switches
# over NNIs.  If FALSE, all the neighbors of a switch, including other
# switches and connected hosts, will be shown.  The default value is TRUE.
# The value of this resource is shown in fvmap via the Options pulldown menu.
#
# *** Note: This resource is only used by pre ForeView 4.1 releases.
#
# Applications that retrieve this resource: fvmap.
#
# Fvmap.NNIsOnly: TRUE
# Fvmap.pollInterval: this resource specifies the polling interval for the
# standalone map in seconds. The standalone map polls the discovery server
# in every 'Fvmap.pollInterval' seconds to update the statuses of switches
# and links displayed on the map. It defaults to 600 seconds(10 min.).
#
# Applications that retrieve this resource: fvmap.
#
# Fvmap.pollInterval: 600
# Fvmap.pollFrequency: this resource specifies the frequency with which
# fvmap asks discovery server for newly discovered switches.
#
# eg.:  if Fvmap.pollFrequency is set to 3, fvmap will query the discovery
#      server for newly discovered switches during every 4th polling cycle.
#      where each polling cycle occurs after 'Fvmap.pollInterval' seconds.
#
# This resource defaults to 5, i.e., fvmap will query for new switches on
# every 6th polling cycle.
#
# Applications that retrieve this resource: fvmap
#
# Fvmap.pollFrequency: 5
#
```

```
# ShowReserved: this resource takes a boolean value 'TRUE' or 'FALSE'.  If
# TRUE, then the applications that provide lists of channels will include
# the reserved channels 5, 14, and 15 in their lists.  If FALSE, those
# channels will not be included.  The default is FALSE.
#
# Applications that retrieve this resource: fvgraph*, fvlog*.
#
# ShowReserved: TRUE
# ConfirmDialog: this resource takes a boolean value 'TRUE' or 'FALSE'.  If
# TRUE, then the application fvchan will ask via a pop-up dialog box for
# confirmation before automatically adjusting bandwidth and/or creating
# Originating & Terminating paths. If FALSE, these dialog boxes will not
# appear.  The default is TRUE.
#
# Application that retrieve this resource: fvchan
#
# ConfirmDialog: FALSE
# ConfirmPMP_PVCs: this resource takes a boolean value 'TRUE' or 'FALSE'.
# If TRUE, then the application fvchan will ask via a pop-up dialog box for
# confirmation before creating Point to MultiPoint PVCs.  If FALSE, this
# dialog box will not appear.  The default is TRUE.
#
# Application that retrieves this resource: fvchan
#
# ConfirmPMP_PVCs: TRUE
# FvChan.ConfigureUPC: this resource take a boolean value 'TRUE' or 'FALSE'. If
# TRUE, then user could configure and select UPC Contract through fvchan. If
# FALSE, user could only select UPC Contract through fvchan. The default is TRUE.
#
# Application that retrieve this resource: fvchan
#
# FvChan.ConfigureUPC: TRUE
# Fvovmon.Tracing: this resource takes a boolean value 'TRUE' or 'FALSE'.  If
# TRUE, then fvovmon will execute with full tracing on.  The tracing
# information is sent to $FOREVIEW_HOME/tmp/fvovmon.log.<pid>.  The default
# is FALSE.  Using this resource is equivalent to passing fvovmon the -t
# flag.
#
# Application that retrieves this resource: fvovmon
#
# Fvovmon.Tracing: FALSE
# Fvovmon.PollNetInterval: this resource takes an integer that specifies
# the amount of time between subsequent polls of a switch in the network.
# Using this resource is equivalent to giving fvovmon the -a flag.  See
# the fvovmon manual page for more information.
#
# Application that retrieves this resource: fvovmon
#
# Fvovmon.PollNetInterval: 900
# Fvovmon.PollDBInterval: this resource takes an integer that specifies
# the amount of time between subsequent polls of the OVw database.
# Using this resource is equivalent to giving fvovmon the -pdb flag.  See
# the fvovmon manual page for more information.
#
# Application that retrieves this resource: fvovmon
#
# Fvovmon.PollDBInterval: 3600
# Fvovmon.PollSwitchStatusInterval: this resource takes an integer that
# specifies the amount of time between subsequent queries to the discovery and
# status daemon for changes in the status of managed switches.  Using this
# resource is equivalent to giving fvovmon the -ssi flag.  See the fvovmon
# manual page for more information.
#
# Application that retrieves this resource: fvovmon
#
# Fvovmon.PollSwitchStatusInterval: 30
# Fvovmon.PollHostStatusInterval: this resource takes an integer that
# specifies the amount of time between subsequent queries to the discovery and
# status daemon for changes in the status of managed ATM-connected devices.
# Using this resource is equivalent to giving fvovmon the -hsi flag.  See the
# fvovmon manual page for more information.
#
# Application that retrieves this resource: fvovmon
#
# Fvovmon.PollHostStatusInterval: 600
# Fvovmon.PollLinkStatusInterval: this resource takes an integer that
# specifies the amount of time between subsequent queries to the discovery and
# status daemon for changes in the status of managed ATM links.  Using this
# resource is equivalent to giving fvovmon the -lsi flag.  See the fvovmon
# manual page for more information.
#
# Application that retrieves this resource: fvovmon
#
# Fvovmon.PollLinkStatusInterval: 900
# Fvovmon.RemoveInterval: this resource takes an integer that specifies
# the amount of time an object in the OVwdb is "dead" before it is
# removed from the map.  Using this resource is equivalent to giving fvovmon
# the -r flag.  See the fvovmon manual page for more information.
#
# Application that retrieves this resource: fvovmon
#
# Fvovmon.RemoveInterval: 86400
# Fvovmon.ReceiveTrap: this resource takes a boolean value.  If set to false,
# then fvovmon does not add the IP address of the net-management station to
# the trap destination list on the managed switches.  Thus, this management
# status will not be registered with the switches to receive traps.  Using
# this resource is equivalent to giving fvovmon the -NT (no trap) flag.  See
# the fvovmon manual page for more information.
#
# Application that retrieves this resource: fvovmon
#
# Fvovmon.ReceiveTrap: TRUE
# FVAccessDevices: this resource takes a comma-separated list of arbitrary
# identifiers.  Each identifier is a string that can be used to map
# a device type to an icon/symbol name.  (Future enhancements will also
# allow one to associate other properties with each device type, e.g., a
# SNMP System Object Identifier.)
#
# Applications that retrieve this resource: fvovmap, fvsnmdsc
#
# FVAccessDevices: AVA, AVB, AVC
# <DeviceType>.iconName, where <DeviceType> is an FvAccess Device identifier
# defined in the FVAccessDevices resource: this resource maps the device type
# to an icon name.  The iconName is used as the base name for the
# symbol/glyph used in OpenView/SunNet-Manager maps.
#
# Applications that retrieve this resource: fvovmap, fvsnmdsc
#
# AVA.iconName: ava
# <DeviceType>.sysOid, where <DeviceType> is an FvAccess Device identifier
# defined in the FVAccessDevices resource: this resource identifies a device
# type with a System Object Identifier.
#
# Applications that retrieve this resource: fvovmap, fvsnmdsc, fvmap.
#
# AVA.sysOid: 1.3.6.1.4.1.999.99
# <DeviceType>.frontPanelApp, where <DeviceType> is an FvAccess Device
# identifier defined in the FVAccessDevices resource: this resource maps
# a device type to a front panel application executable.
```

```
#
# Applications that retrieve this resource: fvpanel
#
# AVA.frontPanelApp: /usr/fore/foreview/bin/fvava
# <DeviceType>.subTypeOid, where <DeviceType> is an FvAccess Device
# identifier defined in the FVAccessDevices resource: this resource
# maps a device type to a subType object identifier for fvdsd.  Fvdsd can
# then retrieve from the device not only its sysOid, but also its subType
# Oid.
#
# Applications that retrieve this resource: fvdsd
#
# AVA.subTypeOid: 1.3.6.1.4.1.1.2.3.4.5.6.0
# <switch-name>/<port>.deviceType, where <switch-name> is the DNS name of
# a switch, <port> is the BNP representation of a port (see Appendix of
# ForeView manual for BNP port mappings): this resource maps a port on a
# switch to a given device type, as defined in the FVAccessDevices resource
# explained above.  Along with the <DeviceType>.iconName resource, this
# allows a user to explicitly define an icon to use to represent an end-point
# device on a ForeView-OpenView or ForeView-SunNet Manager map.
#
# Applications that retrieve this resource: fvovmap, fvsnmdsc
#
# switch1/1C3.deviceType: AVA
# <switch-name>/<port>.mapLabel: this resource maps a port on a switch to a
# label, given as the value of this resource.  The label will be used as
# the label on a port in the Front Panel Application (fvasx) and in the
# ForeView-OpenView and ForeView-SunNet-Manager applications.  However,
# the label is over-written on the port or on the maps if or when the port
# on the given switch has a valid signalling path established on it, and
# the end-point IP address / DNS hostname of the signalling path is available.
# To ALWAYS use the label (regardless of signalling status), set the
# resource "AlwaysOverrideLabels" to "TRUE".  See below.
#
# Applications that retrieve this resource: fvasx, fvovmap, fvsnmdsc
#
# switch1/1C3.mapLabel: VideoFeed1
# <switch-name>/<port>.ipAddress: this resource maps a port on a switch to a
# an IP address, given as the value of this resource.  The IP address refers
# to the address of the device connected to the given port.  This resource
# is read only if the remote IP address registered by signalling has not
# been configured properly.
#
```

```
# Application that retrieves this resource: fvdsd
#
# switch1/1C3.ipAddress: 10.11.12.13
# <switch-name>/<port>.remotePort: this resource maps a port on a switch to
# a remote port on a connected switch, given as the value of this resource.
# The remote port is in the Board-Netmod-Port (BNP) format: e.g., 1A1, 1B5,
# 2A4, etc.  This resource is read only if the
# <switch-name>/<port>.ipAddress resource has also been specified and is
# used (see the description for the resource above) by fvdsd.
#
# Application that retrieves this resource: fvdsd
#
# switch1/1C3.remotePort: 1B1
# AlwaysOverrideLabels: this resource takes a boolean value.  When set to
# a TRUE value, port labels set with the resource
# "<switch-name>/<port>.mapLabel" will ALWAYS be used, even when a valid
# IP address / DNS hostname for the port has been discovered via signalling
# on the port.  The default value is FALSE.
#
# Applications that retrieve this resource: fvasx, fvovmap, fvsnmdsc
#
# AlwaysOverrideLabels: FALSE
# Fvovmap.PollInterval: this resource takes an interger that specifies
# the amount of time between subsequent synchronizations of the OVw database
# and the symbols shown on the current map.  Using this resource is equivalent
# to specifying the -p argument on the command-line to 'fvovmap'.
#
# Application that retrieves this resource: fvovmap
#
# Fvovmap.PollInterval: 900
# Fvovmap.LinkStatusProp: this resource takes a true or false indicator (True,
# 1, Yes, etc. all mean TRUE).  When set to TRUE, fvovmap runs in "Link Status
# Propagation" mode.  In this mode, the status of a switch symbol on the
# "ATM Networks" submap is derived from the status of the center diamond
# switch symbol in the switch's submap AND the status of the links from that
# center diamond switch symbol.
#
# Application that retrieves this resource: fvovmap
# PreferSigType: this resource takes one of "SPANS", "UNI30", or "UNI31" as a
# recognized value.  This resource specifies how host information should be
# shown when there are multiple signalling paths from a switch to the host.
# For a complete explanation of the selection algorithm, see the ForeView
# manual.
```

```
#
# Applications that retrieve this resource: fvsnmdsc, fvovmon, fvasx
#
# PreferSigType: UNI30
# PreferSigVPI: this resource takes an integer as a value.  This resource
# specifies how host information should be shown when there are multiple
# signalling paths from a switch to the host.
# For a complete explanation of the selection algorithm, see the ForeView
# manual.
#
# Applications that retrieve this resource: fvsnmdsc, fvovmon, fvasx
#
# PreferSigVPI: 1
# PreferRemoteIPAddrs: this resource takes a comma-separated list of IP
# addresses or IP ranges.  A range is specified using either "*" to mean all
# value subcomponents (1-255), or "x-y" to mean all integers between x and y
# inclusive.
# For a complete explanation of the selection algorithm, see the ForeView
# manual.
#
# Applications that retrieve this resource: fvsnmdsc, fvovmon, fvasx
#
# PreferRemoteIPAddrs: 169.143.243.7-250, 10.11.*.14, 122.234.33.11
# UseMgmtStatus:
# Fvds.UseMgmtStatus:
# Fvasx.UseMgmtStatus:
# Fvovmon.UseMgmtStatus:
# Fvovtrapd.UseMgmtStatus: these resources take a true or false indicator
# (True, 1, Yes, etc. all mean TRUE).  If "UseMgmtStatus" is set to true, then
# all of fvovmon, fvovtrapd, and fvasx run in a mode in which every port which
# has its "PortManagementStatus" variable set to true is managed, whether or
# not hardware carrier or signalling is up or down on that port.
# Alternatively, one can specify individual applications to run in this mode.
#
# Applications that retrieve this resource: fvovmon, fvovtrapd, fvasx.
# Fvds.hostname: defines the DNS name of the host on which the discovery
# and status (fvds) daemon is running.  Applications that need to retrieve
# information from the daemon use this resource to determine where the
# daemon is running.  In general, if this resource is not defined, or the
# fvds daemon on the specified host cannot be reached, applications
# attempt to contact a daemon on the local host.
#
# Applications that retrieve this resource: fvov*, fvsnm*, fvinv, fvmap,
# fvupgrad.
#
# Fvds.hostname: localhost
# Fvds.port: defines the TCP port on which the fvds daemon listens for
# client connect requests.  The default value is 7890.
#
# Applications that retrieve this resource: fvov*, fvsnm*, fvinv, fvmap,
# fvupgrad.
#
# Fvds.port: 7890
# Fvds.pollNNIDevices: this resource takes an integer, interpreted in seconds.
# This resource specifies the interval for polling all known switches for
# their statuses.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.pollNNIDevices: 30
# Fvds.pollNNILinks: this resource takes an integer, interpreted in minutes.
# This resource specifies the interval for polling all known NNI links for
# their statuses.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.pollNNILinks: 3
# Fvds.pollUNIDevices: this resource takes an integer, interpreted in minutes.
# This resource specifies the interval for polling all known UNI devices
# (ATM-connected devices that are not switches) for their statuses.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.pollUNIDevices: 10
# Fvds.pollUNILinks: this resource takes an integer, interpreted in minutes.
# This resource specifies the interval for polling all known links to UNI
# devices for their statuses.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.pollUNILinks: 30
# Fvds.discInterval: this resource takes an integer, interpreted in minutes.
# This resource specifies the interval over which all known switches, their
# links, and connected hosts are "discovered" -- i.e., all information about
# these devices are retrieved from the switches/hosts.
#
```

```
# Application that retrieves this resource: fvdsd
#
# Fvds.discInterval: 15
# Fvds.discNoUNIs: this resource takes a boolean value.  When set to TRUE, no
# UNI devices or links are discovered by fvdsd.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.discNoUNIs: FALSE
# Fvds.discNoUNIDevices: this resource takes a boolean value.  When set to
# TRUE, no UNI devices are discovered by fvdsd.  I.e., the link information to
# the UNI devices is discovered and monitored, but information about the
# endpoint is not discovered or monitored.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.discNoUNIDevices: FALSE
# Fvds.removeInterval: this resource takes an integer, interpreted in minutes.
# This resource specifies the time that a switch must be recorded as down
# before its status is changed to "removed".
#
# Application that retrieves this resource: fvdsd
#
# Fvds.removeInterval: 3
# Fvds.IPList[0-20]: this resource takes a comma-separated list of ip
# addresses or hostnames as its value.  The value 0-20 identifies these hosts
# as belonging to a special list of devices <n> that should be discovered
# and/or polled by fvdsd at a different rate than the other (unidentified)
# devices.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.IPList[0-20]: host1, switch2, device3, ipaddr4
# Fvds.pollIPInterval[0-20]: this resource takes an integer, interpreted in
# minutes.  This resource specifies the interval that the devices in list <n>
# should be polled for their statues, where <n> is one of 0, 1, 2, ..., 20.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.pollIPInterval[0-20]: 10
# Fvds.discIPInterval[0-20]: this resource takes an integer, interpreted in
# minutes.  This resource specifies the interval that the devices in list <n>
# should be discovered, where <n> is one of 0, 1, 2, ..., 20.  "Discovery" of
# a device means that the fvdsd retrieves all the information about the device
# that it can.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.discIPInterval[0-20]: 10
# Fvds.discInListOnly: this resource takes an boolean value.  When set to
# TRUE, no NNI devices besides those explicitly listed in the discSwitches
# argument/resource are discovered or polled.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.discInListOnly: FALSE
# Fvds.logFileArchiving: this resource takes a boolean value.  When set to
# TRUE, the log file DS.log.<pid> generated by fvds will be periodically
# archived and compressed, according to the other Fvds.logFile* resources
# defined below.  The default value is FALSE.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.logFileArchiving: FALSE
# Fvds.logFileArchiveDir: this resource takes a string that specifies a
# directory in which to place archived versions of the DS.log.<pid> files.
# Its default value is unset, which means that the archived files are not
# moved from $FOREVIEW_HOME/tmp.  Note that the directory MUST be a complete
# absolute pathname, not a relative pathname.
#
# Application that retrieves this resource: fvdsd
#
# Fvds.logFileArchiveDir: /tmp
# Fvds.logFileCompressCmd: this resource takes a string that contains a
# command to use to compress the contents of archived log files.  The
# command may contain a placeholder "%f" which will be substituted with
# the log file's filename before the command is executed.  The default value
# for this resource is unset.
#
# Application that retrieves this resource: fvdsd
#
# On UNIX, a typical setting is:
# Fvds.logFileCompressCmd: /usr/local/bin/gzip %f
# On WinNT, a typical setting is:
# Fvds.logFileCompressCmd: C:\bin\pkzip %f
# Fvds.logFileMaxAge: this resource takes an integer, interpreted in
# seconds.  Setting this resource allows the user to define the maximum
# age of the DS.log file before it is archived.  The minimum value that
# can be set is 900 (equivalent to 15 minutes).  The default value is 86400
# (i.e., 1 day).
#
# Application that retrieves this resource: fvdsd
#
# Fvds.logFileMaxAge: 86400
# Fvds.logFileMaxSize this resource takes an integer, interpreted in
# kilo-bytes.  Setting this resource allows the user to define the maximum
# size of the DS.log file before it is archived.  The minimum value that
# can be set is 10 (i.e., 10 Kbytes).  The default value is 1024 (i.e., 1
# Mbyte).
#
# Application that retrieves this resource: fvdsd
#
# Fvds.logFileMaxSize: 1024
# FvinvLogFile: this resource takes a filename as its value.  This resource
# specifies where fvinv should store version information.
#
# Application that retrieves this resource: fvinv, fvsupp
#
# FvinvLogFile: /usr/fore/foreview/log/fvinv.log
# Fvhelp.tmpDir: this resource takes a directory pathname as its value.
# It is the directory where the ForeView online help facility creates
# temporary HTML documents, as needed.  Note that if your browser is
# Netscape, and you are running it on a remote machine, this directory
# must be NFS-mounted on the remote machine where Netscape is running,
# and with the same path on both machines; otherwise the remote Netscape
# will be unable to load the temporary file for viewing.
#
#if NT
#Fvhelp.tmpDir: C:\TMP
#elseif UNIX
#Fvhelp.tmpDir: /tmp
#endif
# Fvhelp.browser: this resource takes the name of an executable file
# (either full path name or relative, full path name preferred for
# efficiency) that you wish to use as your Help browser.
#if NT
#Fvhelp.browser: netscape.exe
#elseif UNIX
#Fvhelp.browser: netscape
```

```
#endif
# Fvhelp.browserFlags
# Under UNIX, the -install flag is passed to netscape so it will install
# its own colormap.  This is usually necessary for netscape to be usable on
# systems with 8-bit (or less) color.  However, it does cause an
# annoying flashing when switching between netscape windows and other
# windows on the screen, so you can remove the -install flag if you wish.
# Note that this is also controllable via the X resource:
# Netscape*installColormap: True
# but this command line option will override the resource.
#
#if NT
#Fvhelp.browserFlags:
#elseif UNIX
#Fvhelp.browserFlags: -install
#endif
# Fvhelp.netscapeVersion
# If you are using Netscape as your browser, identify the version you are
# using. On UNIX systems, your Help system will work best if you have
# Netscape version 3.0 or later.  That allows remote invocation of netscape,
# targeting a specific window.  Earlier versions allow remote invocation,
# but you can only use an existing window or create a new one each time.
# We have elected to create a new one to avoid inadvertently stealing a
# window that the user has dedicated to some other use, such as mail.
# It is not necessary to define this; on NT it currently does not affect
# the behavior of ForeView, and on UNIX we will query netscape itself
# to determine the version.  However, you can override it with this resource
# if we are somehow obtaining the wrong value.
#
#if NT
#Fvhelp.netscapeVersion: 3.0
#elseif UNIX
#Fvhelp.netscapeVersion: <determined by running "netscape -version">
#endif
# Fvhelp.iexploreVersion
# If you are using Internet Explorer as your browser, identify the version you
# are using. This is only applicable to NT, as Internet Explorer is not
# currently available under UNIX. Version 3.01 must be specified if your
# Internet Explorer fails to come up on some help invocations (i.e. Port Status
# help fails with an IE error that includes a URL with a # sign near the end).
# Also, you can override it with this resource if you need to avoid this
# behavior in any future IE version.
#
```

```
#if NT
#Fvhelp.iexploreVersion: 3.01
#endif
# Fvhelp.httpRoot: this resource takes the root part of a URL as its value.
# If specified, ForeView's online help facility will attempt to obtain
# documents from a Web server relative to the specified location, rather
# than attempting to load local files.  This allows you to put your help files
# on one central Web server and access them from everywhere.  For example,
# if the document requested is "gif/forelogo.gif", and this resource is
# NOT set, fvhelp will attempt to load the file
# "file:$FOREVIEW_HOME/fvhelp/gif/forelogo.gif".  If this resource is set
# to, for example, "//www.mycompany.com/FVHELP" (don't specify the quotation
# marks), then fvhelp will attempt to load the URL
# "http://www.mycompany.com/FVHELP/gif/forelogo.gif".
#
# Fvhelp.httpRoot: <no default>
# Fvpanel.httpServer: this resource specifies server hostname (and,
# optionally, server port) for use by Fvpanel for those Front Panels that are
# World Wide Web-based (e.g., CellPath 90, CellPath90E, and CellPath 300
# devices). The resource should be of the form <hostname>[:<port-number>].
# The port-number is optional if the front panel server is listening at
# the default http port (80). For example, if this resource is set to
# "mars", and you try to start the Front Panel for a CellPath 90 (from either
# the command line or the map), then ForeView will attempt to contact the
# server at port 80 on host "mars".  If the resource is set to "mars:9000",
# then ForeView will attempt to connect to the server at port 9000 on host
# "mars".  The server must be running and waiting for connections prior to
# any attempt to start a Front Panel.
#
# Fvpanel.httpServer: <no default>
```

CHAPTER 4 Network Discovery

The discovery process collects the information used to generate a graphical representation of the ATM network. *ForeView* utilizes a discovery and status server application initiated by **`fvds`**, which launches a daemon process **`fvdsd`** that discovers *ForeRunner* switches, NNI and UNI links, and the endpoints of NNI and UNI links in an ATM network. There are two tasks associated with **`fvdsd`**:

- First, it discovers the network elements and polls the information to keep its own internal cache up-to-date.
- Second, it makes the network topology and status information available to clients. Because this information is made available to clients through a TCP socket, the clients and the server can be distributed across multiple machines to distribute load on the various systems.

4.1 How the Discovery and Status Server Works

The discovery and status server application **fvdsd** maintains an internal cache of information that reflects the current topology and status of the ATM network. The accuracy of the information in the cache depends upon the various polling intervals given in the arguments to **fvds**. The shorter an interval, the more accurate the information. However, shorter polling intervals mean a higher load on the system on which **fvdsd** is running, and a greater amount of traffic on the network and on the managed devices.

NOTE The executable **fvdsd** is launched by a start-up script **fvds**. Users should not launch **fvdsd** directly.

4.1.1 Discovery Arguments

The arguments for **fvds** reflect a distinction between discovery and polling. Discovery is the retrieval of a complete set of device information, including the device name, interface information, ATM (SPANS) address, device type, enclosure identifier, board number (for switch fabrics), system object identifier and all network module information, and connectivity information, including all link / port statuses, and all signalling path information (both SPANS and UNI 3.x).

The following are command-line arguments for network discovery:

-discInterval *minutes* Instructs **fvdsd** on the discovery interval, where *minutes* is the interval in minutes between subsequent discoveries of a switch, its NNI and UNI links and neighbors of the switch in the database. The default is 15 minutes.

-discSwitches *list* Instructs **fvdsd** to discover a list of ATM switches and all their neighbors, where *list* is a comma separated list of IP addresses or hostnames, enclosed in single or double quotes. (As a resource value, the list need not be enclosed in quotes.) The list of devices is used as a list of seeds for discovery and polling of the network at start-up time.

-discNoUNIs Instructs **fvdsd** that UNI signalling paths and UNI-connected devices need not be discovered or status polled, because clients will not be interested in this information.

-discNoUNIDevices Instructs **fvdsd** that UNI signalling paths should be discovered and polled, but the endpoint devices of UNI signalling paths should not be discovered or polled.

-discInListOnly Instructs **fvdsd** to limit the discovery to a set of switches. By default, **fvdsd** is greedy, discovering and monitoring everything that is ATM-connected. Using the **-discInListOnly** flag, only switches (and not their neighbors) in the list are discovered.

-t This option turns on tracing for **fvdsd** The tracing output goes to the file **/usr/fore/foreview/tmp/fvdsd.log.PID**, where **PID** is the process identification number.

-port The number of the port on which **fvdsd** should listen for client connection requests. The default is 7890.

4.1.2 Polling Arguments

Polling is updating of the status of an object in **fvdsd's** internal cache. Objects include switches (or, more generally, NNI devices), NNI links, UNI links, and UNI-connected devices. The status of an NNI device is determined by the success of an SNMP query to the device. The status of a UNI device is determined by the success of either an SNMP query or a ping to the device. The status of a link is a combination of the status of the signalling paths on the link and the hardware carrier status, as reported by the switch.

The following are command-line arguments for network polling:

-pollNNIDevices *seconds* Instructs **fvdsd** to poll each cached NNI device's status, where *seconds* is the polling interval in seconds. The default is 1 minute.

-pollUNIDevices *minutes* Instructs **fvdsd** to poll each cached UNI device's status, where *minutes* is the polling interval in minutes. The default is 10 minutes.

-pollNNILinks *minutes* Instructs **fvdsd** to poll each cached NNI link's status, where *minutes* is the polling interval in minutes. The default is 3 minutes.

-pollUNILinks *minutes* Instructs **fvdsd** to poll each cached UNI link's status, where *minutes* is the polling interval in minutes. The default is 30 minutes.

4.1.3 Seeding the Discovery

To discover the ATM network and to build up the database, **fvds** must be “seeded” with a switch or switches. The seeds for network discovery can be provided using the **-discSwitches** command line argument. The list of switches given to **-discSwitches** must be a comma-separated list of switch names, given as a single command line argument -- i.e., enclosed in double or single quotes.

If no seed switches are provided via the command line, **fvdsd** looks in **$FOREVIEW_HOME/tmp/fvdsd.db** for a list of seed switches, one per line. (As **fvdsd** discovers switches, it updates this file with the switch names.) In some cases, **fvdsd** may be started up without any seed switches and without a seed file. In this case, **fvdsd** will not discover any devices until a client seeds the cache with a switch hostname.

While it runs, **fvdsd** generates a log file that contains the changes detected in the network topology and status. The log file is found in **$FOREVIEW_HOME/tmp/DS.log.<pid>**, where **<pid>** is the process identifier of **fvdsd**. Note that after initial network discovery, only changes to the network are logged in this file.

NOTE

This record of observed network changes can be useful for monitoring the status of the entire network.

4.1.4 Limiting the Discovery and Polling

You can limit the amount of information discovered and polled by **fvdsd** by using the arguments **-discInListOnly**, **-discNoUNIs**, **-discNoUNIDevices**, and the arguments **-IPListn** in combination with **-pollIPIntervaln** and **-discIPIntervaln**, and by setting polling intervals to the special value 0. In the default operating case, **fvdsd** discovers and polls all devices and links that it can find.

However, to only monitor ATM switches, specify **-discNoUNIs** to instruct **fvdsd** to not discover or poll any UNI links or their connected endpoints. To only discover and poll switches, their NNI links, and their UNI links, but not their connected UNI-endpoints, specify **-discNoUNIDevices** on the command line (or via the configuration file, as described later in the chapter).

You can set a discovery interval to 0 to instruct **fvdsd** to not discover (and thus poll) certain types of devices. For example, setting **-discInterval** to 0 turns off all default discovery of all devices (NNI and UNI devices and NNI and UNI links).

4.1.4.1 Customized Discovery and Polling

Custom lists of devices that should be discovered and polled differently than the default devices can be configured. Up to 21 lists (numbered 0 through 20) of IP addresses or DNS hostnames can be specified, and **fvdsd** can be instructed to discover and poll each list of devices separately. Each list is a comma-separated list, provided as a single argument -- i.e., enclosed in double or single quotes. Discovery and polling of devices in these lists includes only discovery and polling of the devices themselves -- not their links, signalling paths, nor connected neighbors.

NOTE

A custom list can be used to specify certain devices that should not be discovered or polled by the default discovery and polling operations. By specifying a list of devices and setting its discovery and polling intervals to 0, certain devices are essentially marked as devices that should not be monitored.

The following are additional command-line arguments that can be used to limit and customize network discovery and polling:

-IPList*n list* Defines a list of devices, called *n list*, that should be discovered and polled according to the intervals given in the command-line arguments **-pollIPIntervaln** and **-discIPIntervaln**. Only the devices themselves will be discovered and polled. The links, signalling paths, and connected neighbors will not be discovered or polled. These options can be used to monitor important devices more often than other “default” devices. Where *n* is an integer from 0 through 20, and *list* is a comma-separated list of IP addresses or hostnames.

-pollIPInterval*n minutes* Instructs **fvdsd** to poll the list of devices defined in the **-IPListn** option, where *n* is an integer from 0 through 20, and *minutes* is the polling interval in minutes. The default is 30 minutes.

-discIPInterval*n minutes* Instructs **fvdsd** to discover the list of devices defined in the **-IPListn** option, where *n* is an integer from 0 through 20, and *minutes* is the discovery interval in minutes.

Various parameters of the polling operations, including SNMP community names and timeout values of SNMP requests, are configured in **$FOREVIEW_HOME/conf/fvsnmp.conf** or **~/.fvsnmp.conf**.

NOTE

The careless configuration of SNMP values can cause **fvdsd** to operate slowly when it tries to communicate with non-reachable switches or hosts.

4.1.5 Configuration File Resources

All of the command-line arguments described in this chapter can be provided in one of the *ForeView* configuration files, either in **$FOREVIEW_HOME/conf/foreview** or **~/.foreview**. For most of the command line-line arguments, the resource names are the same as the arguments and the specifier is "Fvds." For example, the **-discSwitches** command-line argument can be provided in the configuration file as:

```
Fvds.discSwitches: comma-separated, list, of, switches
```

And, the **-port** command-line argument is given as:

```
Fvds.port: <port-number>
```

Please refer to Chapter 3, Configuring ForeView, for more information about these configuration file resources.

4.1.6 Alternative Discovery Mode

You can run **fvdsd** in an alternative discovery mode by specifying **-UseMgmtStatus** on the command line (or via the configuration file). The **-UseMgmtStatus** mode allows you to explicitly define the set of ports on switches that should be managed, and those that should be ignored. This can be useful when you want to manage ports for which no signalling exists and hardware carrier status should be monitored and displayed. (In the default mode, if no hardware carrier exists on a port, then no information about the port is recorded by **fvds**.)

In **-UseMgmtStatus** mode, **fvdsd** discovers a link for every port on every switch for which the MIB variable **portManagementStatus** is set to 1 (managed).

NOTE

The **-UseMgmtStatus** mode requires that the switch's *ForeThought* software be version 4.1.0 or later. (For switches running software earlier than 4.1.0, all ports will be managed as if the **portManagementStatus** variable were set to 1.) For ports with the **portManagementStatus** variable set to 2 (un-managed), no information about the port will be discovered or polled by fvdsd. This mode is usually set not only in **fvdsd** but also in other *ForeView* tools, for example, **fvasx**, and the *ForeView* for OpenView daemon **fvovmap**.

4.2 Scaling Network Discovery

Enhancements to *ForeView* improve the scalability of the management platform by allowing the network manager to execute multiple copies of the discovery and status daemon (**fvdsd**) in parallel on multiple machines. To take full advantage of this scheme, the network manager needs to carefully partition the network, and then assign each copy of fvdsd to discover and monitor one partition.

Improving the scalability of *ForeView* by running multiple **fvdsd's** concurrently, with each **fvdsd** monitoring a single partition, provides the following benefits:

- It allows the network administrator to actively monitor a larger ATM network while minimizing management resources.
- It allows the network administrator to use machines with moderate network bandwidths, running **fvdsd's** concurrently, to monitor the ATM network because the amount of management traffic is distributed over several links.

4.2.1 How Scaling Works with OpenView/NetView

To implement scalability, multiple copies of **fvovmon** (*ForeView's* status and monitoring daemon) and **fvovtrapd** (*ForeView's* trap handler) run on the same machine where the OpenView database (**ovwdb**) is running. Each instance of **fvovmon** is associated with a single **fvdsd** and retrieves the network topology and status of a partition, and keeps **ovwdb** up-to-date with the current status of the partition.

The OpenView database (**ovwdb**) thus becomes the central repository of the ATM network information. The OpenView map then can display the aggregate network information collected by all the **fvdsd's**. This distributed approach to ATM network monitoring is illustrated in Figure 4.1. More information on **fvovmon** and **fvovtrapd** is provided in Chapter 5.

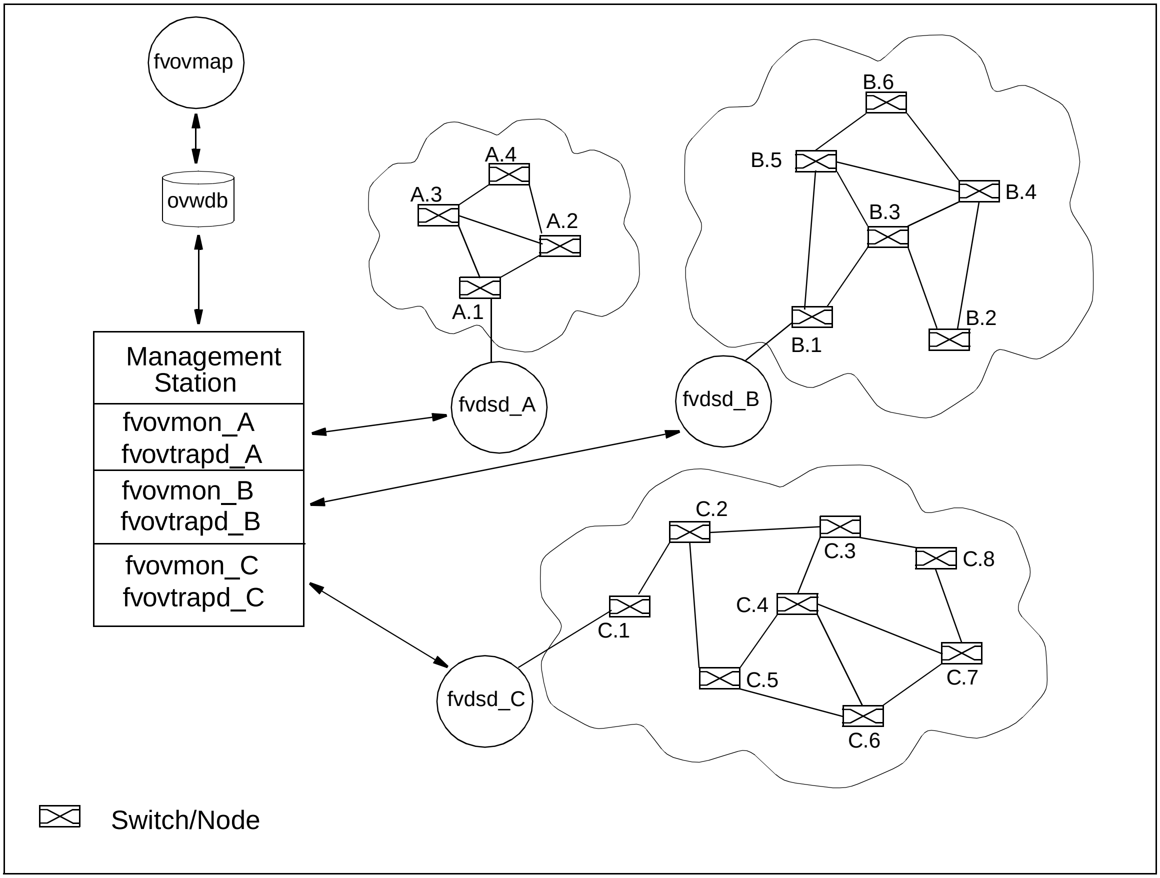


Figure 4.1 - Distributed Network Monitoring

4.2.2 How Scaling Works with the Stand-alone Map

The stand-alone map application is not able to show the entire network because it can show only a map view containing all the switches monitored by a single **fvdsd**. For example, if B.1 is monitored by fvdsd_B and C.2 is monitored by fvdsd_C, while the stand-alone map application is connected to fvdsd_B, no information about C.2 can be displayed because fvdsd_B is not aware of C.2.

NOTE

The stand-alone map application can disconnect from one **fvdsd** and connect to another **fvdsd**. The switches monitored by another **fvdsd** are shown by switching map views.

4.2.3 How To Deploy Scaling

Currently, the **`-discInListOnly`** feature is in place to limit **`fvdsd`** to monitoring just a portion of the ATM network. The **`-discInListOnly`** feature instructs **`fvds`** to limit the discovery to a set of switches. With the feature enabled, **`fvdsd`** will not discover new switches additional to the switches that are given to it at start up time.

Using **`-discInListOnly`**, the ATM network can be neatly partitioned into subsections, each being monitored by an **`fvdsd`** running on a specific machine. For each **`fvdsd`** deployed, the user must provide a list of switches that the **`fvdsd`** is supposed to monitored. See section 4.1.4 for more information on the **`discInListOnly`** feature.

NOTE

A new switch added to the network will not come into the client's view automatically, because no **`fvdsd`** would be aware of the switch for discovery. When a new switch is added to the ATM network, at least one **`fvdsd`** must be brought down and restarted with the new switch added to its list of switches to monitor.

4.2.4 Monitoring Edge Switches

When an ATM network is partitioned, and there are links connecting those partitions, the monitoring of the partitions by the various **`fvdsd`** instances must be done carefully. To see the connections between two partitions, one of the two **`fvdsd's`** monitoring the partitions must monitor the edge switches of the other partition, i.e., there must be some monitoring overlapping for the edge switches. A partitioned network with connected edge switches is illustrated in Figure 4.2.

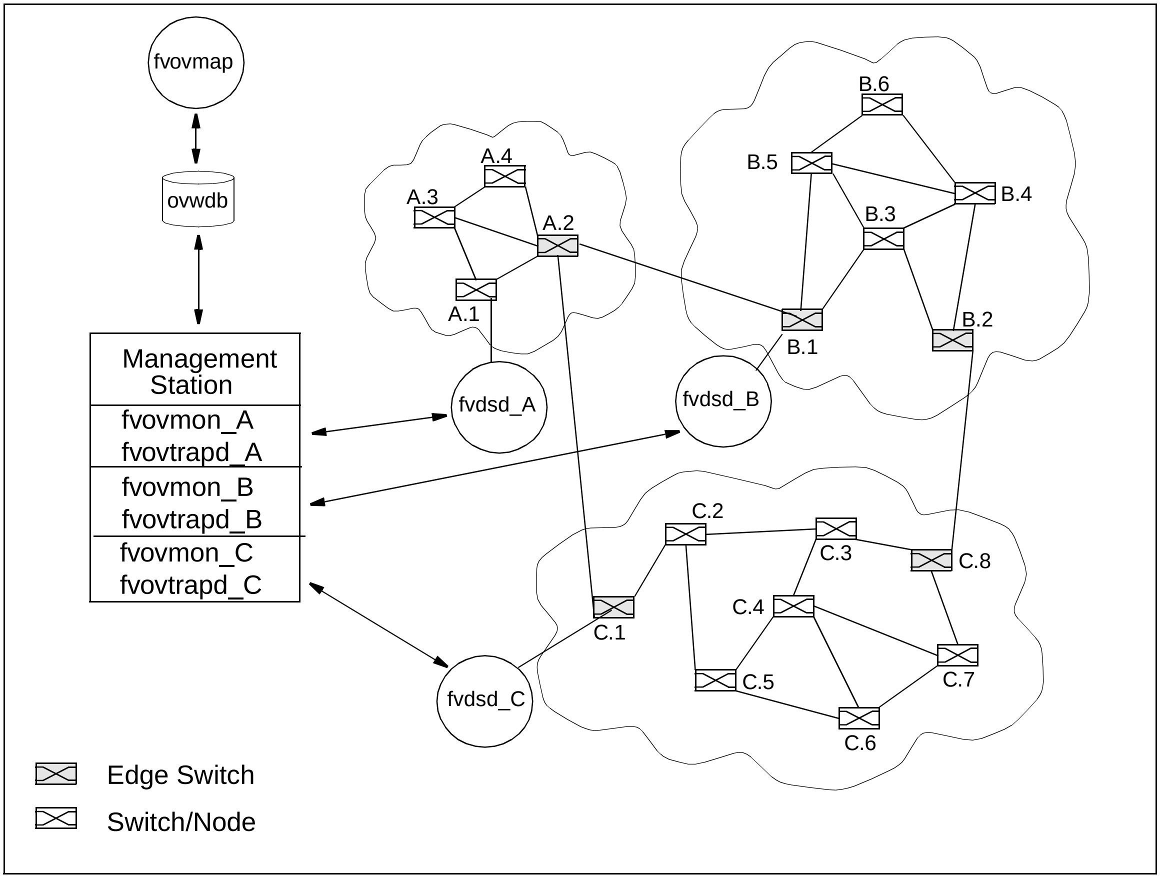


Figure 4.2 - Partitioned ATM Network with Edge Connections

For example, in the three logical network partitions A, B, and C in Figure 4.2, switches A.2, B.1, B.2, C.1, and C.8 are the edge switches of the partitions. In order for the clients to see the connections, one of the **fvdsd** instances must monitor the other two partition's edge switches. The administrators who set up the partitions must carefully generate the switch lists in order to be able to monitor all the connections as well as to minimize monitoring overlapping.

4.2.5 Enabling Scaling

The daemons **fvovmon** and **fvovtrapd** read the resource **Fvds.hostname** and **Fvds.port** to find out the location of **fvdsd**. To enable starting up multiple copies of **fvovmon** and **fvovtrapd**, one additional option is added to the command line of **fvovmon** and **fvovtrapd**:

```
[-host <fvdsd_machine>] [-port <fvdsd_port>]
```

This option tells the daemons from which **fvdsd** each of them should be getting the information and facilitates running multiple **fvovmon** daemons and multiple **fvovtrapd** daemons on the same machine.

To have multiple copies of **fvovmon** and **fvovtrapd** start when ovstart is run, there must be multiple lrf registration files for each of the daemons. At installation, the registration files for the daemons are generated dynamically, one for **fvovmon** and one for **fvovtrapd**, for each instance of **fvdsd** that is running. The registration files are stored in the **$FOREVIEW/OV/lrf** directory.

CHAPTER 5 Running *ForeView* with HP OpenView and NetView for AIX

This chapter provides information on how to run *ForeView* under HP OpenView and NetView for AIX. *ForeView* includes a status and monitoring daemon, *fvovmon*, a mapping application, *fvovmap*, and a trap handler, *fvovtrapd*, that handles FORE-specific traps. The daemon *fvovmon* contacts the *ForeView* discovery and status daemon (*fvdsd*) to retrieve the ATM network topology and status, and keeps the OpenView database (*ovwdb*) up-to-date with the current status of the ATM network. The mapper *fvovmap* places the ATM objects in the database into an OV map, which shows the status of hosts, links, and switches. The trap handler *fvovtrapd* monitors the received traps and updates the database. Thus, the state of the network is quickly reflected in the OpenView database and the map. These applications, illustrated in Figure 5.1, are all tightly integrated into HP OpenView and NetView.

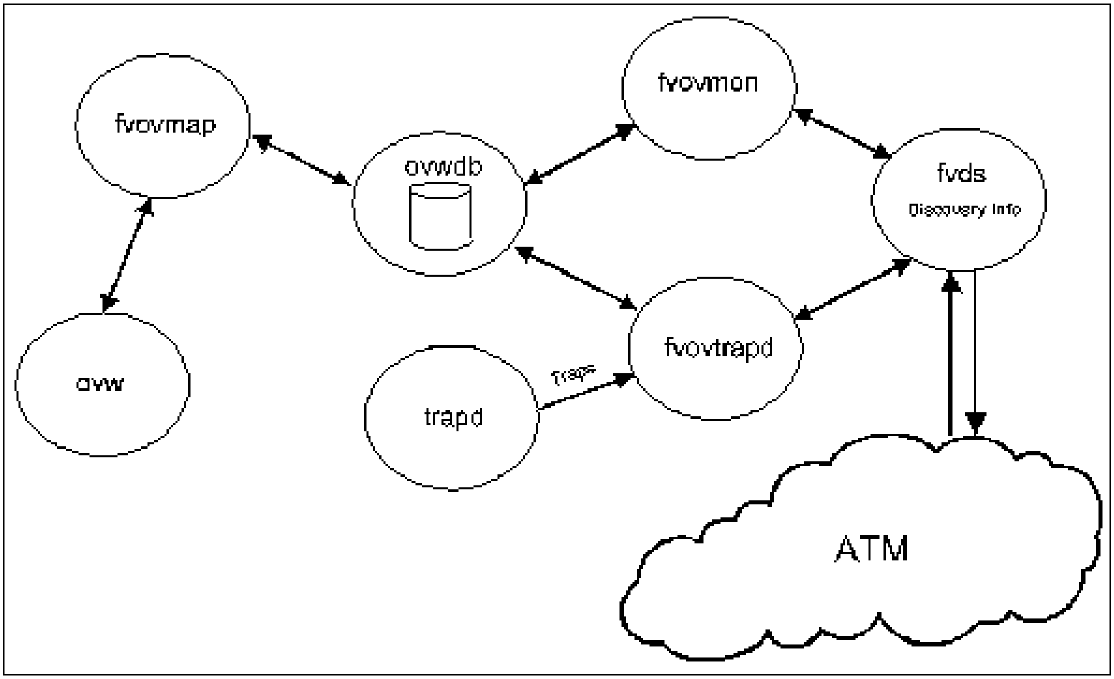


Figure 5.1 - *ForeView's* Integrated Processes

5.1 Starting *ForeView* with OpenView/NetView

ForeView is integrated with HP OpenView and NetView for AIX. To run OpenView or NetView, log in as a regular user. Prior to running *ForeView*, the following directories should be in the search path:

- **`/usr/OV/bin`** for NetView, or
- **`/opt/OV/bin`** for OV 4.x on Solaris and HPUX-10.x.

NOTE

For OpenView version 4.x, make sure that **`/opt/OV/lib`** is in the **`LD_LIBRARY_PATH`** variable, and that **`/opt/OV/bin`** is in the **`PATH`** variable.

If this has not been done, modify the appropriate system configuration files. Then, OpenView or NetView can be run by typing the following command at the system prompt:

```
ovw <ENTER>
```

NOTE

A new *ForeView* menu selection in the OpenView and NetView main menu bar appears to the right of the other OpenView / NetView menu items.

5.1.1 Installation Note for AIX 4.1 with NetView 4.x

The installation of *ForeView* at a location other than **`/usr/fore/foreview`** on AIX 4.1, with Netview 4.x, may bring up the following messages:

```
WARNING: fvds did not successfully initialize.
WARNING: You will have to start it using ovstart.
```

In that case, the following steps are recommended:

```
1. ps -aef | grep nvsecd
2. kill -9 <process id of nvsecd>
3. ps -aef | grep ovspmd
4. kill -9 <process id of ovspmd>
5. ovstart
```

5.2 The Discovery Process

This is accomplished by the routine polling of the network by **fvovmon**, and subsequent updating of the network database. In addition, **fvovtrapd** handles trap messages from network devices and updates the network database.

5.2.1 Polling Network Elements

A *ForeView* for HP OpenView daemon, **fvovmon**, is responsible for retrieving network topology and status information from the *ForeView* discovery and status daemon **fvdsd** and updating the OpenView database with the information. **fvovmon** periodically queries the **fvdsd** for the status of switches, links, hosts, signalling paths, and ATM-access devices, as well as querying for changes to the network topology.

The polling period for each type of network element can be set in the ForeView configuration file or via the command line. These values should be coordinated with values given for polling periods in fvdsd.

After the switch, network module, port, and signalling information is retrieved, it is parsed, and the database is updated. If an interswitch connection is discovered, the remotely connected switch is added to the polling list. After all switches in the polling list are polled, the updated list of polled switches is written to a file.

NOTE

To increase *ForeView's* scalability, a change has been made in *ForeView* 4.3. The process **fvovmon** no longer learns switches by searching the **ovwdb** for switches discovered by **netmon/ipmap**. Therefore, if you have multiple ATM clouds (disconnected ATM networks), at least one switch from each cloud must be specified in the **FvdsdiscSwitches** resource.

Every 15 minutes (by default), **fvovmon** checks the database for all its managed objects. Each object is checked for the last time it was observed. If an object has not been updated for more than four consecutive polling cycles, that object is declared "unreachable" and the symbol is turned red. If an object has not been updated for more than 24 hours, that object becomes "unmanaged" by **fvovmon** (which has the effect of removing the symbol from the map).

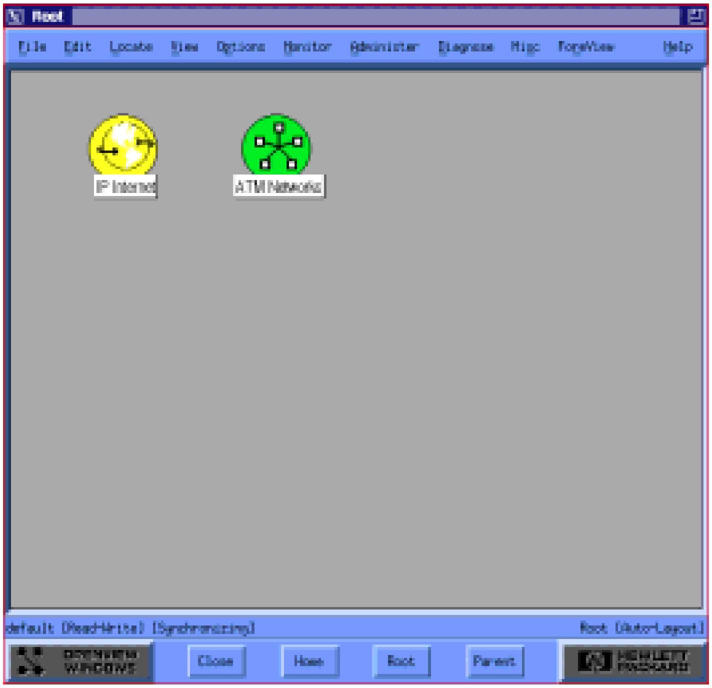
Periodically, **fvovmap** does a complete database synchronization with the symbols currently shown. Unmanaged objects have their symbols removed. The user can force a database synchronization by using the **Options -> Foreview: Synchronize Map** pulldown.

5.3 *ForeView*'s ATM Map

ForeView's **`fvovmap`** is an application that is integrated under HP OpenView Windows. **`fvovmap`** reads ATM topology data and displays it in a four-level map format.

5.3.1 Root Level Submap

In the **Root Level** submap, a symbol for the entire ATM network is presented together with the IP internet symbol. The color of the symbol represents the status of the ATM network.



default [Read-Write] [Synchronizing]
Root [Auto-Layout]

Figure 5.2 - Level 1 Submap - Root Level

5.3.2 ATM Networks Submap

Double-clicking on the ATM Networks symbol launches the **ATM Networks** submap. This submap displays all the switches and the interswitch connections that exist in the managed network.

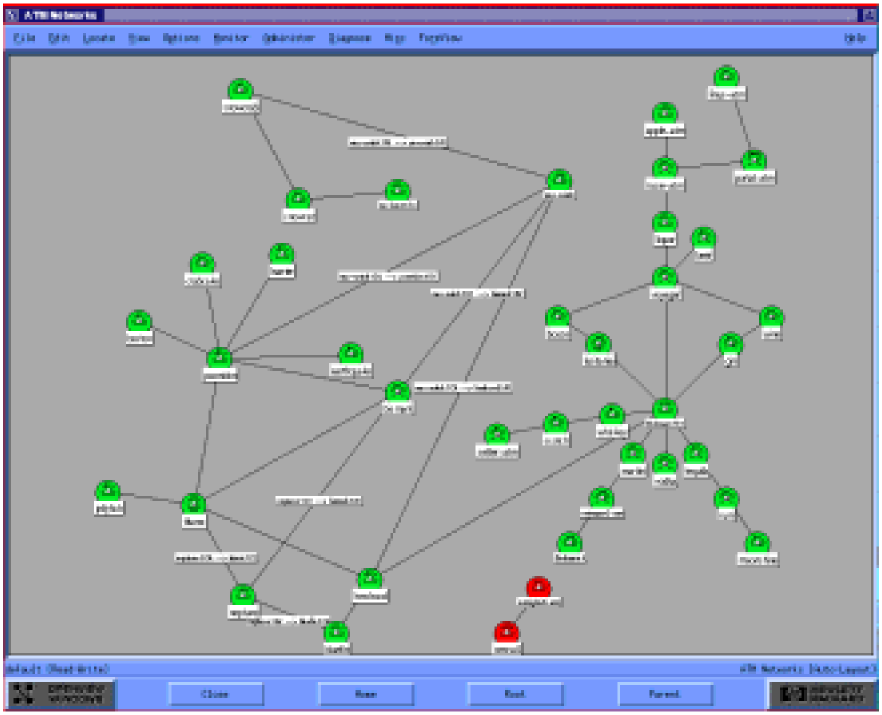


Figure 5.3 - Level 2 Submap - ATM Networks

5.3.3 Switch Connections Submap

Double-clicking on a switch symbol brings-up the **Switch Connections** submap. In this submap, the switch is displayed in the center of the screen and all the attached devices (hosts, switches, ATM-access) are displayed around it in a star layout.

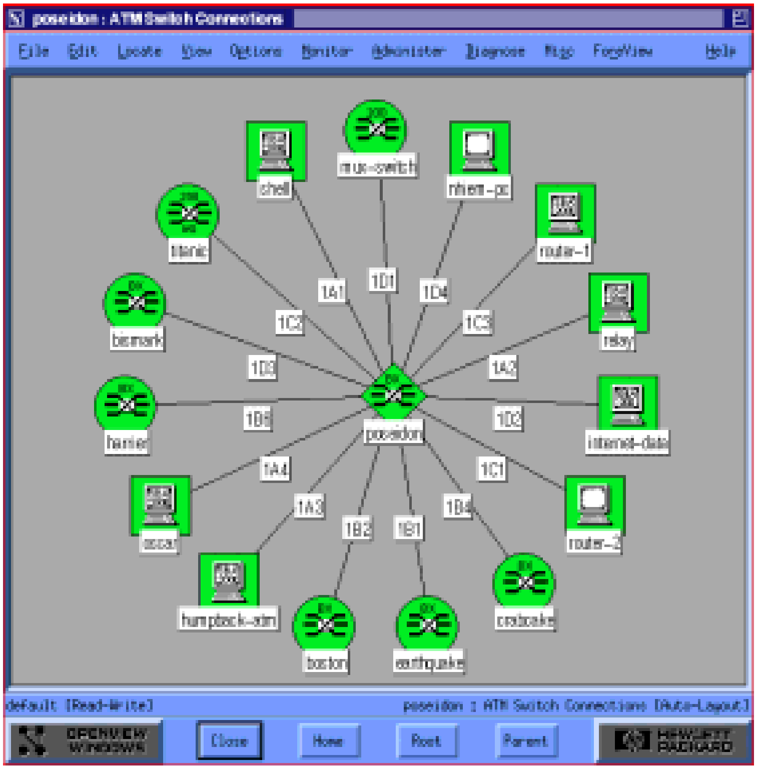


Figure 5.4 - Level 3 Submap - Switch Connections

5.3.4 ATM Links Submap

A line between switch icons in the ATM Network Submap indicates that a connection exists between those switches. Double click on the line to bring up a submap with all unidirectional links between the two switches. Each link label is composed by the two ends of the physical link, **`switch1-name:np --> switch2-name:np`**. The NP notation is derived from the network module identifier (A-D) plus the actual port number (see Port Indicators, section 7.7). The arrow indicates the direction.

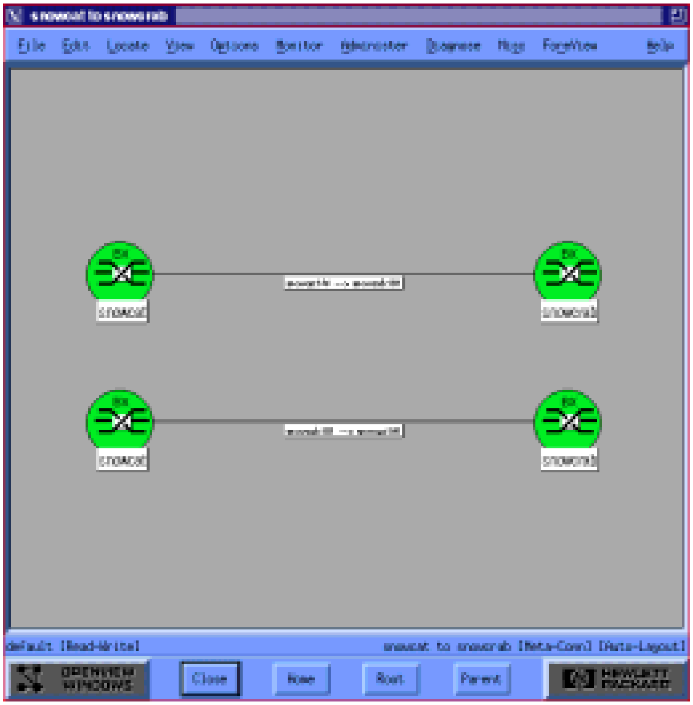


Figure 5.5 - ATM Links Submap

5.3.5 Link Information Submap

As previously stated, a line between switch icons in the ATM Network Submap indicates that a connection exists between those switches. When you double click on the line, a submap with all unidirectional links between the two switches is called up. To verify the type of signalling paths and hardware carrier connections that exist for a link, double click on the link. Valid signalling path types are UNI 3.x and SPANS.

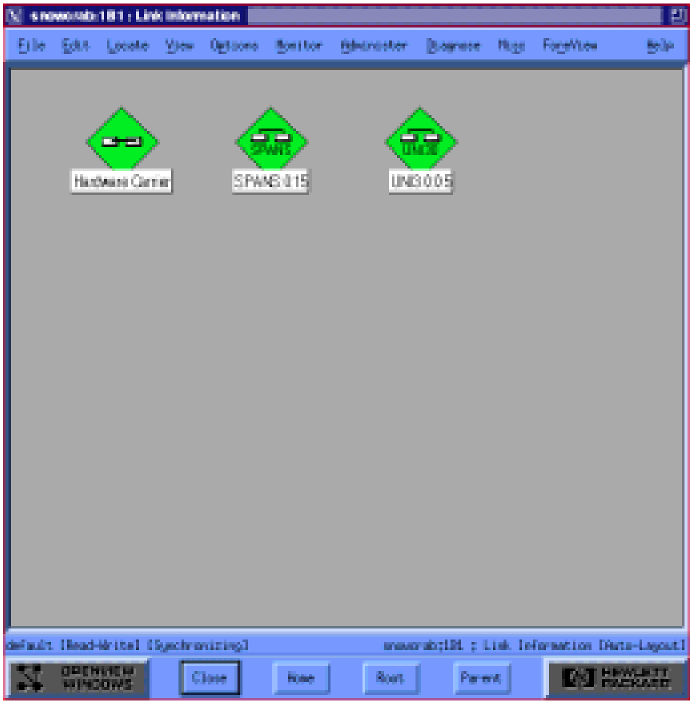


Figure 5.6 - Signalling Paths Submap

5.3.6 Fabrics Submap

Double-clicking on an ASX-1000 switch symbol brings up the **Switch Fabrics** submap. An ASX-1000 can be populated with up to four fabrics. This submap displays the valid switch fabrics in the enclosure.

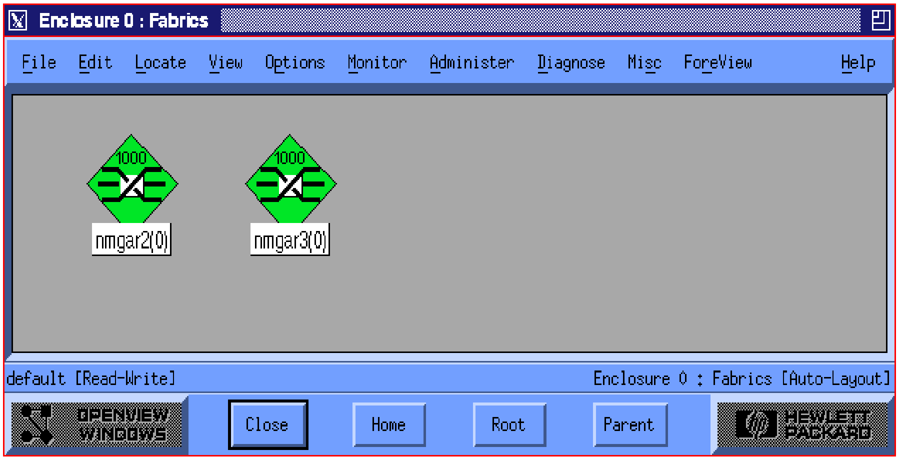


Figure 5.7 - Switch Fabrics Submap

5.3.7 How Status Colors are Derived

The color of the ATM object (switch, host, link, or ATM-access device) represents its status. When a host symbol becomes red, that means that the host can not be reached (pinged) from the management station.

The status of a link is based upon the combined status of the signalling paths and line status in the link's submap. A black link indicates that all signalling paths over the link are operational. A link of any other color indicates that one or more symbols in the link's submap is down. Please refer to the OpenView / NetView manuals for a discussion of how status combinations are implemented.

If the color of a switch is not green, it indicates that the switch (or one or more fabrics in the switch) is down.

Interswitch links may become red when the interswitch connection is down. Because the down interswitch link symbol resides within a meta-connections submap, the line on the ATM connections map that is the parent for this submap will change color, indicating a warning. This line is a component symbol, and gets its status from all the symbols that reside in its submap. Therefore, it will become cyan, yellow, orange, or red depending on the number of underlying unidirectional links that went down.

The color of the ATM networks symbol in the **Root Level** submap represents the status of the entire ATM network. The symbol is blue if there are no ATM objects in its submaps. It is green if all switches and interswitch links in the map are OK. It becomes yellow, cyan, orange, or red if there are some ATM switches or interswitch links that are down.

NOTE

When a host or a link to a host is down, and the symbol color changes to red, the color of the switch symbol in the **ATM Networks** submap does not change. It stays green as long as the switch itself is up and running. This is done to distinguish between different severities of failure. From the ATM network perspective, the failure of a switch or an interswitch link is much more important than the failure of a host or a link to the host. Therefore, the status of a host does not propagate to the top level ATM Networks symbol.

Interswitch connections are also displayed on the **Switch Connections** submap. All links in this submap are labeled by the switch's port **NP** to which they are connected. The color of the link indicates the signalling status. The color of the remote node indicates whether the node can be reached (via SNMP or ping) from the management station. All labeled links may be selected for graphing utilization or statistics. For more information about the graphing application see the Tracking Network Usage chapter and the **fvgraph** commands.

5.3.8 Location Symbols

ForeView running under OpenView supports a feature that allows you to create a “location” symbol that represents multiple symbols in a single location in the managed network. When created, other symbols from a submap then can be cut and pasted in a related submap launched from the “location” symbol. This submap is referred to as the “location submap”.

The status of the location symbol is derived from the combined status of the symbols in a location submap. The use of the location symbol increases the usability of OpenView in a large network because multiple symbols are represented by a single symbol on the original submap and the complete network representation is partitioned into multiple submaps.

NOTE Symbols can be created from the "Location" symbol class only, on the "ATM Networks" submap only.

5.3.8.1 How Location Symbols are Implemented

The following are requirements for the successful implementation of location symbols:

- The creation of location symbols, and the automatic creation of the location submap, is supported in the "ATM Networks" submap only.
- Location symbols in the "ATM Networks" submap can be deleted only if the associated location submap is empty.
- Symbols from a submap are cut-and-pasted onto a location submap.
- Symbols from a location submap can be cut-and-pasted back to a regular submap or to another location submap.
- The status of links to and from symbols moved from one submap to another are updated using the model implemented by HP OpenView's **`ipmap`** process in the "IP Networks" submap hierarchy.
- Assignment of symbols to location submaps is maintained when **`ovw`** is restarted.

NOTE If a symbol is cut from one submap, it must be pasted onto another. If the symbol is not pasted in a timely manner (i.e., before **`fvovmap`** starts a synchronization cycle), then **`fvovmap`** will paste the symbol onto the "ATM Networks" submap.

NOTE This feature does not support the dynamic creation of new symbols. Only symbols that have previously been cut from a submap can be added to another submap.

5.3.8.2 Implementation Summary

The implementation of location symbols can be explained in three phases: the start-up, the handling of a cut event, and the handling of a paste event.

5.3.8.2.1 Start-up

Upon start-up, all symbols on the “ATM Networks” submap are retrieved. Next, for each location symbol that exists, the routine caches the location symbol identifier and its corresponding submap identifier in a hash table (the hash table is created dynamically if it does not already exist). This cache is keyed by submap identifier. The cache is useful for maintaining a record of locations symbols and submaps that have been created, as well as for translating submap to symbol identification.

5.3.8.2.2 Symbol Deletion

A delete (or cut) action generates two events: a “deletion verify” event followed by a “delete” event. The deletion verification event gives an application a chance to disallow deletion of certains symbols, such as the deletion of location symbols that do not have empty submaps. All other symbols are allowed to be deleted.

NOTE

When a switch symbol is deleted, link symbols are explicitly deleted in a meta-connection submap.

5.3.8.2.3 Symbol Creation

The second half of a cut-and-paste operation involves creating new symbols in a submap. When the symbol creation event is received, the routine handles the following cases:

- A symbol being created is a location symbol on the “ATM Networks” submap.
- A symbol is being created on a location submap.
- A symbol is being created on the “ATM Networks” submap.

5.4 Map Icons

Map icons provide easy recognition of ATM devices and hosts on the network. An enhancement to *ForeView* 4.1 is a labeling convention to identify different types of *ForeRunner* switches, ATM-access devices, and hosts more readily.

5.4.1 ATM Switches

Each switch icon in the ATM Networks submap, as well as the Switch Connections and ATM Links submaps, is labelled with the type of device; e.g., “200” means ASX-200, and “BX” means ASX-200BX.

Only switches with a known IP hostname (or address) will be presented on the **ATM Networks** submap. This is the only way further SNMP queries (that are based on IP datagrams) can be performed on this switch.

5.4.2 Hosts

The labels of switches and hosts are their IP hostnames (or addresses) on their ATM interface. For example, if a switch has two interfaces, Ethernet and ATM, the IP hostname on the Ethernet interface is “cat”, and on the ATM interface is “cat-atm”. The label “cat-atm” will be used as the switch label in the **ATM Networks** submaps, while either “cat” or “cat-atm” will be used in the IP Internetwork Map for the same switch.

A host icon also may contain a label identifying the type of adapter in use, if the host is equipped with a FORE Systems’ adapter product such an SBA-200 or HPA-200.

NOTE

It is recommended that you have an IP host naming convention for a network device that has at least two interfaces and carries IP traffic. One convention is for IP hostnames on all interfaces to have a common basic name which enables an easy association between the IP map representation and the ATM map representation of the same network element (switch, host, or ATM-access device).

5.5 The Discovery Process

The discovery process generates a graphical representation of the ATM network. This is accomplished by the routine polling of the network by **fvovmon**, and subsequent updating of the network database. In addition, **fvovtrapd** handles trap messages from network devices and updates the network database.

5.5.1 Polling Network Elements

A *ForeView* for HP OpenView daemon, **fvovmon**, is responsible for retrieving network topology and status information from the *ForeView* discovery and status daemon **fvdsd** and updating the OpenView database with the information. **fvovmon** periodically queries the **fvdsd** for the status of switches, links, hosts, signalling paths, and ATM-access devices, as well as querying for changes to the network topology.

The polling period for each type of network element can be set in the ForeView configuration file or via the command line. These values should be coordinated with values given for polling periods in fvdsd.

After the switch, network module, port, and signalling information is retrieved, it is parsed, and the database is updated. If an interswitch connection is discovered, the remotely connected switch is added to the polling list. After all switches in the polling list are polled, the updated list of polled switches is written to a file.

NOTE

To increase *ForeView's* scalability, a change has been made in *ForeView* 5.0. The process **fvovmon** no longer learns switches by searching the **ovwdb** for switches discovered by **netmon/ipmap**. Therefore, if you have multiple ATM clouds (disconnected ATM networks), at least one switch from each cloud must be specified in the **FvdsdiscSwitches** resource.

Every 15 minutes (by default), **fvovmon** checks the database for all its managed objects. Each object is checked for the last time it was observed. If an object has not been updated for more than four consecutive polling cycles, that object is declared “unreachable” and the symbol is turned red. If an object has not been updated for more than 24 hours, that object becomes “unmanaged” by **fvovmon** (which has the effect of removing the symbol from the map).

Periodically, **fvovmap** does a complete database synchronization with the symbols currently shown. Unmanaged objects have their symbols removed. The user can force a database synchronization by using the **Options -> Foreview: Synchronize Map** pulldown.

5.5.2 SNMP Traps

The **fvovtrapd** daemon receives a FORE System’s trap from an SNMP device, then filters and translates the trap. A trap is an unsolicited report sent from an agent that often signifies some unexpected error condition. The traps are then logged in the event log file. When **fvovtrapd** receives one of these traps, it updates the database accordingly.

For example, if a switch detects that an interswitch connection becomes non-operational, the switch sends an asxSwLinkDown trap to the network management station. The **fvovtrapd** daemon receives the trap, checks that it is a *ForeRunner* switch trap, decodes the trap message, checks the database, and updates the database if needed. If that link was already down in the database (e.g., discovered in an earlier polling cycle), no updates are required.

To verify that every trap is valid, **fvovtrapd** asks **fvdsd** to update its information about the switch/link that generated the trap.

In all *ForeRunner* switches, a table of trap destinations exists. When the switch detects a change in the operational status of one of its ports, it sends a trap to all network management stations that appear in the trap destination list. This list is represented by a MIB table, and can be written using SNMP set messages. When **fvovmon** detects a new switch in the network and polls it, it sets an entry in the switch's trap destination table for the IP address of the machine on which **fvovmon** is running. From this point on, traps may be received from this switch, and changes in the status and topology of the network will be reflected on the **fvovmap** almost immediately.

For more information about MIB objects that are used in the discovery of the ATM network, please refer to **fore-switch.mib** located in the **/usr/fore/foreview/mibs** directory.

5.6 Launching *ForeView* Tools from HP Openview

ForeView includes several utilities which run in combination with OpenView / NetView. These tools allow you to monitor the ATM Network, take inventory of ATM equipment, create connections, and track network usage. You can also launch a separate ATM Network map.

These tools are integrated into the **`ForeView`** menu within OpenView / NetView. Also, the tools can be run outside of OpenView / NetView via the command line.

5.6.1 Selecting ATM Devices and Hosts

To use *ForeView* to track network usage, simply select what you want to track in the **ATM Networks** submap, the **ATM Switch Connections** submap, the **Inter-switch Connections** submap, or a labeled link. Then pull down the **`ForeView`** menu; and select one of the menu items.

5.6.2 *ForeView* Tools

The following options are available from the pull-down **`ForeView`** menu after making a selection from one of the maps:

Front Panel View Provides a graphical representation of an actual *ForeRunner* switch, including the number and type of network modules installed in the switch, the status of the ports on each of these modules, and the Internet name for the Ethernet Port and Control Port. See Chapter 8 for more information about the Front Panel.

Allows you to monitor network links and devices and provides a detailed view of a FORE Systems' LAN-access devices such as PowerHubs, ES-3810s, ES-3850s, and the LAX-20. See the *ForeView* Device Manager manual for information about the front panels for these devices.

AMI Starts a telnet session to the switch called up from Front Panel. By default, log in as “asx” to access the built-in administrative tools.

Graph... Select one of the four menu items: switch ports, switch paths, switch channels, or hosts. This method works for graphing network usage for switches, links, and hosts in your network. See Chapter 10 for more information on Graphing.

Log... Select one of the four menu items: switch ports, switch paths, switch channels, or hosts. This method works for logging network usage for switches, links, and hosts in your network. See Chapter 10 for more information on Logging.

Config Paths/Channels... Starts the Virtual Channel/Path tool for the creation of Paths (Through Paths, Signalling Paths), PVCs, and Smart PVCs. See Chapter 8 for more information on the creation of Virtual Channels.

Trace Paths/Channels Starts the Channel Trace tool. See Chapter 11 for more information on Channel Trace.

Inventory Starts the Inventory utility. See Chapter 12 for more information on Inventory.

Alternate Map Starts the Stand-alone Map. See Chapter 7 for more information on the Stand-alone Map.

Upgrade Switch Software Starts the FORE switch software upgrade utility.

Call Record Starts the Call and Performance Records collection utilities for billing and maintenance purposes.

OAM Cell Monitor Starts the OAM (Operations and Maintenance) utility to track switch traffic problems.

5.6.3 Selection Options for Graphing and Logging

When selecting a switch for graphing or logging, you are able to choose from all the enabled ports on that switch (or switches), including the control port. The control port is an internal logical port which carries traffic to and from the control processor. The type of traffic generated and received by a switch includes network management (SNMP) traffic.

To graph or log usage by a host, select the host(s) that you wish to track. Tracking usage by specific hosts in your network allows you to track a single user or user group in your network.

In general, when graphing or logging switch options (ports, paths, channels) using the *ForeView* Tools:

- Graph or log switch options from switches selected from the **ATM Networks** submap, the **ATM Switch Connections** submap, and the **Inter-switch Connections** submap.
- Graph or log switch options from links selected in the **ATM Switch Connections** submap and the **Inter-switch Connections** submap.

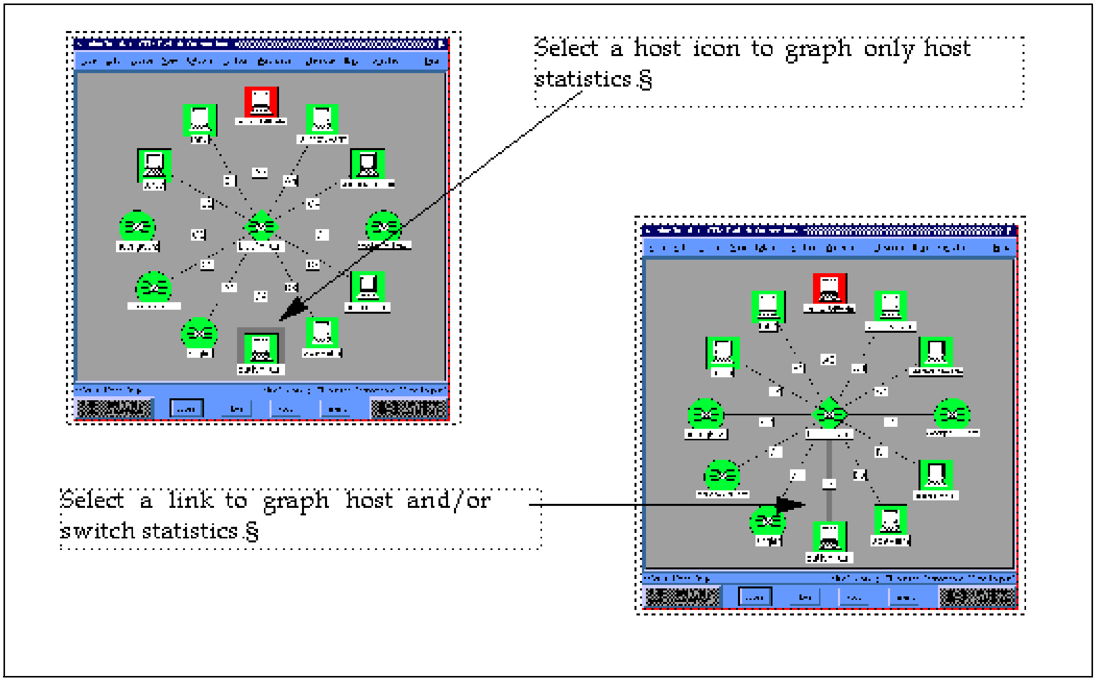
In general, when graphing or logging host statistics using the *ForeView* Tools:

- Select hosts from the **ATM Switch Connections** submap, either by selecting a host icon or by selecting a host-to-switch link.
- When you select a host icon from the *ForeView* map, switch options (ports, paths, channels) are disabled, and only the host option is available.
- Selecting a link between a host and a switch allows you to track the host, and also allows you to track the switch parameters (ports, paths, channels).

Figure 5.8 illustrates the host-to-switch link selection and the host icon selection. In a host-to-switch link, the only the host statistics are available.

NOTE

When a host is connected to a switch and that host is not transmitting IP traffic, the host is identified as *switch port-**bnp*** where **b** is the board, ***n*** is the network module, and **p** is the port on the switch to which the host is attached. If a host is not transmitting IP, **`Graph/Host`** will not work because the graph tool relies on the host to reply to the SNMP agent, which runs on top of IP.



Select a host icon to graph only host statistics.§

Select a link to graph host and/or switch statistics.§

Figure 5.8 - Options for Host Selection

5.7 Threshold Events and Actions with HP OpenView Network Node Manager

5.7.1 Setting Up a Threshold Event

HP OpenView Network Node Manager includes a Data Collector. If you have Network Node Manager, you can use its Data Collector to set up polled thresholds in your ATM network. You can use polled thresholds to watch for conditions in your network. For example, you could monitor a critical link in your network and beep your pager when utilization on the link exceeds 5% for 10 seconds.

NOTE

Operations in this section require HP OpenView Network Node Manager. The Data Collector does not come with the basic HP OpenView SNMP platform. Also note that this section documents steps using Network Node Manager version 3.3. There were subtle changes in the Data Collector and event configuration between Network Node Manager versions 3.2 and 3.3.

5.7.2 Summary of Setting Up a Threshold Event

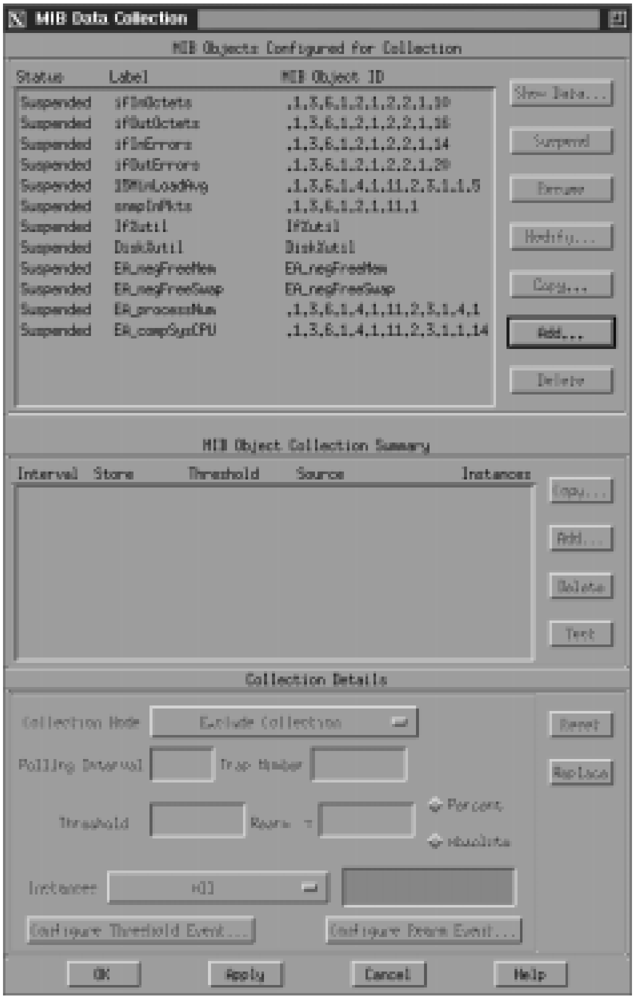
The following is a summary of the steps necessary to set up a threshold event. For users not familiar with HP OpenView's Network Node Manager and Data Collector, a more detailed explanation of these steps follows this summary.

There are three requirements to set up a threshold event:

- Select a MIB variable to monitor.
- Set up the threshold and monitoring interval.
- Attach an action that you want to happen when the condition occurs.

5.7.3 Select a MIB Variable to Monitor

Select OpenView's **`Options / Data Collection & Thresholds: SNMP...`**. You will see a number of standard collectable parameters in the upper list box when the dialog appears, as shown in Figure 5.8, MIB Data Collection Dialog.



Status	Label	MIB Object ID
Suspended	ifInOctets	.1.3.6.1.2.1.2.2.1.10
Suspended	ifOutOctets	.1.3.6.1.2.1.2.2.1.16
Suspended	ifInErrors	.1.3.6.1.2.1.2.2.1.14
Suspended	ifOutErrors	.1.3.6.1.2.1.2.2.1.20
Suspended	15MinLoadAvg	.1.3.6.1.4.1.11.2.3.1.1.5
Suspended	snmpInPkts	.1.3.6.1.2.1.11.1
Suspended	If%util	If%util
Suspended	Disk%util	Disk%util
Suspended	EA_negFreeMem	EA_negFreeMem
Suspended	EA_negFreeSwap	EA_negFreeSwap
Suspended	EA_processNum	.1.3.6.1.4.1.11.2.3.1.4.1
Suspended	EA_compSysCPU	.1.3.6.1.4.1.11.2.3.1.1.14

Interval	Store	Threshold	Source	Instances

Collection Mode: Exclude Collection

Polling Interval:

Trap Number:

Threshold:

Rearm:

○ Percent

○ Absolute

Instances: All

Figure 5.9 - MIB Data Collection Dialog

Create custom objects to be collected (and thresholded) by specifying MIB variables to collect. For example, to monitor an ATM link for 5% utilization, select the **portTransmittedCells** parameter from the FORE enterprise MIB.

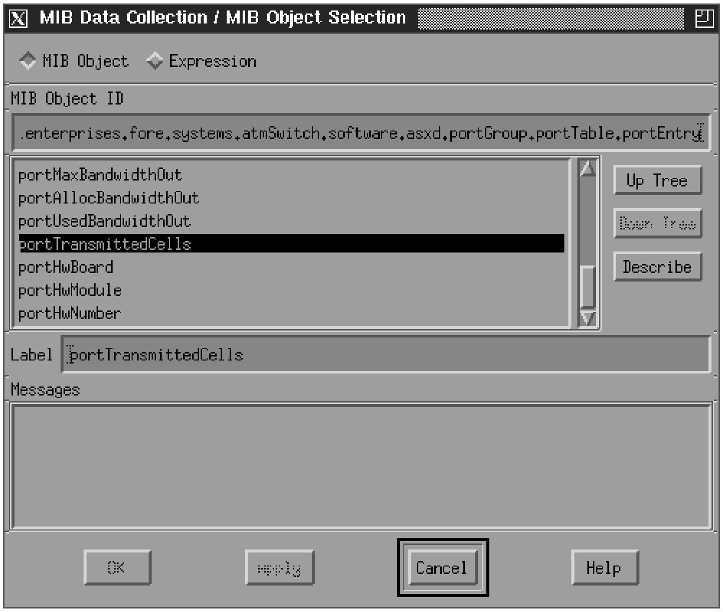
To do this, select the **`Add...`** button in the upper pane. The **`MIB Object`** radio button is selected by default.

NOTE

You can add not only raw MIB objects to track, but also expressions which are formulas involving basic MIB objects. See HP OpenView documentation on **mibExpr.conf** for creating your own custom expressions.

To choose a MIB object, you must navigate the MIB tree to a leaf-node. To choose **portTransmittedCells**, double-click on **`private`**, then on **`enterprises`**, then on **`fore`**, etc., until you have selected **`private.enterprises. fore.systems.atmSwitch.software.asxd.portGroup. portTable.portEntry. portTransmittedCells,`** as shown in Figure 5.9, MIB Object Selection Dialog.

When finished, you should see **portTransmittedCells** selected in the list box and its label in the edit field. Next, select **`OK`**. A second dialog will automatically appear to prompt you for nodes from which to collect information.



MIB Object ID: .enterprises.fore.systems.atmSwitch.software.asxd.portGroup.portTable.portEntry

portMaxBandwidthOut
portAllocBandwidthOut
portUsedBandwidthOut
portTransmittedCells
portHwBoard
portHwModule
portHwNumber

Label: portTransmittedCells

Figure 5.10 - MIB Object Selection Dialog

5.7.4 Set Up Event Thresholds

Type the hostname of the switch from which you are collecting information in the **Source** edit field; for example, **netmgtsw1**. Then select **Add** to add this to the **List of Collection Sources** field.

Next, for **Collection Mode**, make sure **Don't Store, Check Threshold**s is selected. This checks MIB variables for thresholds without collecting them and storing them in local OpenView database files.

Next, specify the polling interval, threshold, and rearm values. In our example, we want to see if average utilization on the link exceeds 5% for 10 seconds. So, the polling interval will be every 10 seconds. Type **10s** into the **Polling Interval** field.

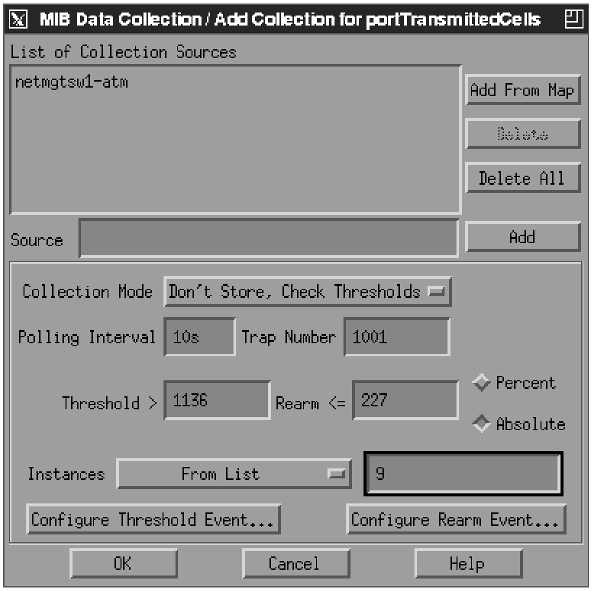
The 5% value depends on the maximum transmission rate for the selected link. This example monitors a 100 Mbps TAXI link. The maximum Cells/Sec on a 100 Mbps TAXI link is 227274. Five percent of this is 1136. Enter **1136** in the **Threshold** field.

To prevent an event from occurring every 10 seconds if the actual utilization goes above 5% and stays there, the OpenView Data Collector allows you to specify a rearm value, below which the parameter must fall before another event is triggered. For example, specifying a rearm value of 1% of the link capacity does not allow a second event to occur until link utilization falls from above 5% to below 1% and then climbs back above 5%. To specify an absolute value rearm at 1%, 1% of the maximum link rate is 227. Enter **227** in the **Rearm <=** field.

Next, specify which instances of the MIB variable to have the threshold occur. There is a separate instance of the **portTransmittedCells** variable for each port on a *ForeRunner* switch. The instance of the variable is indexed by a softport number. For example, on an ASX-200, port B2 is softport 9. So to threshold on **portTransmittedCells** on port B2 of an ASX-200, enter **9** into the **Instances** field and make sure **From List** is the instance type.

Finally, identify the **Trap Number** to use when a trap must be generated when the threshold is exceeded. The default **Trap Number** is 58720263 which is known as the **OV_DataCollectThres** trap. This trap occurs when any generic Data Collector threshold is exceeded.

By default, this generic trap is configured to log a message to the OpenView event log and do nothing else. A custom trap may be created if you want to attach a custom action to a trap that occurs. In OpenView 3.3, custom traps are odd numbers between 1001 and 1999. Enter **1001** in the **Trap Number** field. Your Data Collection configuration screen should now look something like Figure 5.10.



MIB Data Collection / Add Collection for portTransmittedCells

List of Collection Sources: netmgtsw1-atm

Source:

Collection Mode: Don't Store, Check Thresholds

Polling Interval: 10s

Trap Number: 1001

Threshold >: 1136

Rearm <=: 227

◇ Percent

◇ Absolute

Instances: From List — 9

Figure 5.11 - Data Collection for Threshold Trap

5.7.5 Set Up an Action On a Threshold Event

At this point, the Data Collector is configured to collect information from the MIB variable specified and to check against the threshold to see if it is being exceeded. There is still one piece missing. When the threshold is exceeded, the Data Collector generates a trap number 1001, which is currently undefined. You must define this trap and attach an action to it.

To define the trap, select **`Configure Threshold Event...`** from the MIB Data Collection dialog.

NOTE

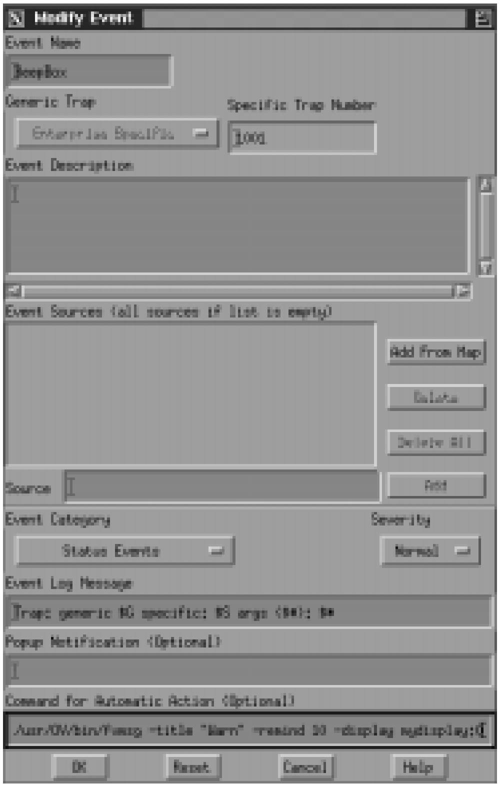
Because an event for trap number 1001 is not defined yet, you will see a warning box. You need to add trap number 1001 manually.

Select **Add...** to create the new event type and bring up the Modify Event Dialog, shown in Figure 5.11. Create a new **Event Name**. In this example, we will not beep a pager, but will show a box which beeps at the user until acknowledged. Let's call this event **BeepBox**. Enter **BeepBox** in the **Event Name** field. Enter the new event number, **1001,** in the **Specific Trap Number** field. There is an example script which comes with *ForeView* called **fvmsg** (/usr/OV/bin/fvmsg). This script takes a number of arguments. In the **Command for Automatic Action** field, enter the following:

/usr/OV/bin/fvmsg -title “Warn” -remind 10 -display mydisplay:0

“Link utilization above 5%”

Select **OK** to close the screen. Then select **Apply** in the Event Configuration dialog to add the new event.



Modify Event

Event Name: BeepBox

Generic Trap: Enterprise Specific

Specific Trap Number: 1001

Event Category: Status Events

Severity: Normal

Event Log Message: Trap: generic $G specific: $S args ($#): $*

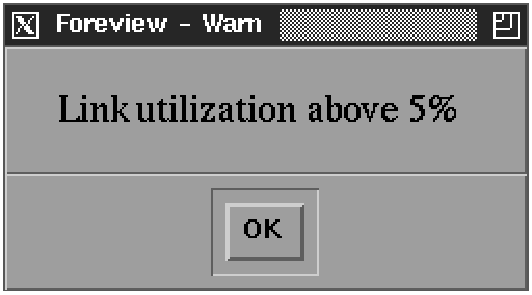
Command for Automatic Action (Optional): /usr/OV/bin/fvmsg -title "Warn" -remind 10 -display mydisplay:0

Event Description
Event Sources (all sources if list is empty)
Add From Map
Delete
Delete All
Source
Add
Popup Notification (Optional)
OK
Reset
Cancel
Help

Figure 5.12 - Modify Event Dialog

Now, everything is configured. The Data Collector is periodically collecting information from the switch, checking against our threshold, and generating a trap (1001) if the threshold is exceeded. On receipt of this internal trap, we have attached an action.

When this trap occurs, a message box will pop up for the user which beeps until acknowledged.



Link utilization above 5%

Figure 5.13 - Threshold Event Trap Message

5.8 Debugging Threshold Events

It is recommended that you force the threshold condition in your network to occur to test out your threshold and action. If you create this condition in your network, and no trap occurs, you will have to see why it is not being generated. You can use the main MIB Data Collection screen to store data in addition to checking thresholds by changing the **`Collection Mode`** to **`Store, Check Thresholds`**.

Then you can examine collected data using the **`Show Data...`** button after selecting the **portTransmittedCells** item in the upper list box to make sure that it is being collected properly and the thresholded condition is occurring as you suspect.

When the Data Collector detects the condition, it sends a trap. You can examine the OpenView event log to check to make sure a trap is received when the condition occurs. If a trap is received, but no action is being taken, examine the configured event for the trap number that shows up in the OpenView event log, trap number 1001 in this example.

5.9 Trap Configuration

Traps are generated whenever a change occurs in the network (for example, when a link goes down, a threshold is exceeded, a new entity is added, etc.). Notification of new traps can be viewed in the Event Categories window. This window has six predefined categories, each with a corresponding button. A change in button color indicates that an event occurred for that category and a corresponding trap has been sent.

NOTE When you click on a button in the Event Categories window, a window listing the events appears.

The six predefined categories are as follows:

Error Events Indicates an inconsistent or unexpected behavior has occurred.

Threshold Events Indicates a threshold has been exceeded.

Status Events Indicates an object or interface status has changed to up or down, or an object or interface has started or stopped responding to ICMP echo requests.

Configuration Events Indicates a change to the configuration of a node.

Application Error Events Indicates an HP OpenView application generated an alarm or alert.

All Events Includes all of the above events and any others in one dialog.

As previously stated, a change in button color indicates that an event occurred. The color of the button indicates the severity of the event. HP OpenView allows you to change the severity of a trap and to create new trap categories. For example, you can change the trap severity of link status (up / down) from **`Warning`** to **`Major`**.

5.9.1 Changing Trap Severity

Use the HP OpenView console to change trap severity. For example, the following steps explain how to change the trap severity of **`Link Down`** from **`Warning`** to **`Major`**.

1. Pull down the **`Options`** menu item and click on **`Event Configuration: SNMP...`**
2. Select **`FORE_ASX`** to view FORE-specific traps.

NOTE

Selecting FORE_ASX will produce a list of traps (Event Name), the Severity classification (Critical, Major, Minor, Warning, Normal), and the Sources.

3. Highlight **`FORE_ASX Link Down`**.
4. Click on the **`Modify`** button to bring up the **`Modify Event`** dialog.
5. Change the **`Severity`** to **`Major`** (pull down the **`Severity`** menu and click on the selection).

NOTE

As an option, you can create a custom pop-up notification or an automatic command response for the trap from this dialog.

6. Click **`OK`** to return to the Event Configuration dialog.
7. To end this process, Click **`OK`** to close the Event Configuration dialog.

5.10 Troubleshooting *ForeView* on HP OpenView

5.10.1 Checking *ForeView* Processes

As with all other HP OpenView background processes, **fvovmon**, should be running whenever *ForeView* is running. Normally, the back ground processes are started by **running ovstart**. Initially, **fvovmon** is started immediately after installing *ForeView* by **ovconfigure**. To verify that **fvovmon** is running, type:

```
ovstatus
```

The result shows you the status of all **ovw** daemons that are supposed to be running, and their status. You should see the following for **fvovmon**:

```
object manager name: fvovmon
behavior:         OVs_WELL_BEHAVED
state:                  RUNNING
PID:                    <pid>
last message:Initialization complete.
exit status:      -
```

If **ovstatus** indicates that there is a problem with **fvovmon**, try to restart **fvovmon** by typing the following as root:

```
ovstart fvovmon
```

Checking the status of **fvovmap** is different, since it is launched by **ovw**. Whenever **ovw** is running, you can check to make sure that **fvovmap** is running using the following command:

On a Hewlett-Packard or Solaris Platform:

```
ps -ef | grep fvovmap
```

5.10.2 Checking Error Logs

All traps that are received by **fvovtrapd** are logged in the events log, **trapd.log**. When changes in status or topology of the ATM network are not reflected in the map, check the following:

- Make sure that changes in status or topology of the network (e.g., a port became operational), are logged as traps from the switch.
- Make sure that changes of status or topology cause updating of the database. You should do that by looking for **fvovtrapd** traps that follow traps from the switch.
- Look for changes of status (color) or topology (links to hosts or switch) on the ATM network submaps. Even if the map does not reflect the change immediately, check it after 2 minutes. That is the default interval in which **fvovmap** checks the database to resynchronize itself.

All errors are logged to application specific log files. For **fvovmon**, the file is **/usr/fore/foreview/tmp/fvovmon.log.<PID>**, where **<PID>** is the process ID. For **fvovmap,** the error log file is **/usr/fore/foreview/tmp/fvovmap.log.<PID>**. Severe errors are displayed as an alert dialog in addition to being logged in the error log file.

5.10.3 Examining the OVW Database

Another important debugging tool is **ovobjprint**, which displays the contents of the **ovw** database. It is useful to print the contents of the database into a file, and then to check that the ATM objects in the database represent the current ATM network topology, as well as checking that the ATM map represents the ATM database objects correctly. For more information about this tool, refer to the HP OpenView man pages and/or manuals.

5.10.4 Deleting the Map Database and Rediscovering

If the map does not appear the way you want it, you may want to restart automatic map generation from scratch. You may want to do this if the discovery process is too slow, and you wish to restart the discovery with a seed file (for one or both of **fvovmon** and **netmon** processes), or when the topology of your entire management domain has changed dramatically.

To restart automatic map generation, enter the following commands:

```
cd /usr/OV/bin/ovstop

rm -rf /usr/OV/databases/openview/*/*

rm -f /usr/OV/log/trapd.log*

rm -f /usr/OV/log/nmevents.*

/usr/OV/bin/ovstart ovwdb

/usr/OV/bin/ovw -fields
```

```
/usr/OV/bin/ovstart -v
```

CAUTION

This deletes not only *ForeView* ATM map information, but ALL OpenView map information. There is no way to delete just ATM map information. See TAC for this.

5.10.5 Creating a Trap Category

Software messages generated by *ForeView* appear in the **Status Events** trap dialog. You can create a new trap classification to log these *ForeView*-generated messages, creating a *ForeView*-specific category for ease of viewing. These traps still will be included in the **All Events** category.

The following steps explain how to create a new trap category.

1. Pull down the **Options** menu item and click on **Event Configuration: SNMP...**
2. Select **OpenView** from the **Enterprise Identification** list.
3. Highlight **FV_Message** in the **Event Identification** window.
4. Click on the **Configure Categories...** button to launch the **Configure Event Categories** dialog.

NOTE

This dialog lists the items seen in the **Event Categories** window.

5. Enter a new category name (**FV Events**, for example).
6. Click the **Add** button to complete this action.
7. Click on the **Close** button.
8. Highlight **FV_Message** in the **Event Identification** window.
9. Click on the **Modify** button.
10. Pull down the **Event Category** menu item and click on the new category just created (**FV Events,** for example).
11. Click on the **OK** button.
12. Click on the **OK** button on the **Event Configuration: SNMP...** dialog.

5.11 Maintenance Commands

5.11.1 Options for fvovmap

The application *fvovmap* displays a map of a *ForeRunner* ATM network as discovered by *fvovmon* under HP OpenView.

The following synopsis lists the various options for *fvovmap*:

```
fvovmap  [-t] [-p interval] [-s session_ID]
```

fvovmap is an application that is integrated under *ovw*(1). It reads ATM topology data created by *fvovmon*(8) and receives ATM topology events which it uses to display the ATM network topology.

The ATM topology is displayed in a hierarchy of submaps that is initially four levels deep: Root, ATM Networks, ATM Switch Connections, and, at level 4, either Fabrics or Signalling Paths. The Root level contains an ATM Networks symbol which reflects the status of the entire ATM network. The ATM Networks level submap shows switches and the links between them. The ATM Switch Connections level submap shows a single switch and all of the hosts and switches attached to that switch. Under an ’enclosure object’ (a ForeRunner ASX-1000 or ForeRunner ASX-BXE switch) on level 3, there is a Fabrics submap that displays all the fabrics in the enclosure. Under each link at level 3, there is a submap that displays all the signalling paths established on that link.

Map Synchronization

fvovmap will synchronize the displayed ATM map with the database created by *fvovmon* under three conditions: at startup, on receipt of a topology-change event from *fvovmon*, and on a regular polling interval (15 minutes) which keeps the ATM map in sync with the database. While *fvovmap* is synchronizing, *ovw* displays a **’Synchronizing’ message**on**the**status**line**of**the-**displayed**ATM**submaps. During synchronization, *ovw* restricts users from deleting symbols and objects.

The **’Synchronizing’ message**will**flash**occasionally**while** *fvovmap* is updating the network map. This is normal behavior. The short periods of synchronization are a result of symbols being deleted and added as *fvovmap* updates the map to reflect the ATM network database.

UseMgmtStatus Mode

fvovmap can be run in an alternative mode called "UseMgmtStatus" mode. See the ForeView manual for more information about this mode. To run *fvovmap* in this mode, place the line:

```
Fvovmap.UseMgmtStatus: TRUE
```

into one of the ForeView resource files.

5.11.1.1 Options

To change options for *fvovmap*, the user must edit the fvovmap registration file in /usr/OV/registration/C.

–t This option turns on tracing for *fvovmap*. The tracing output goes to a file in /usr/fore/foreview/tmp/fvovmap.log.PID.

–p*interval* where *interval* is called the polling interval. Every polling interval, *fvovmap* synchronizes the OVW submaps with the contents of the OVW database. The default value is 900 seconds (15 minutes).

–s*session_ID* where *session_ID* is filled in with $OVwSessionID from an OV registration file when using the distributed launching capabilities of OV 4.0 or later.

5.11.1.2 Files

/usr/OV/registration/C/fvovmap *fvovmap* application registration file.

/usr/fore/foreview/tmp/fvovmap.log.PID Trace file for fvovmap with process id PID.

5.11.2 Options for Status and Monitoring

The daemon *fvovmon* retrieves information about switches, links, signalling paths, and hosts from the *ForeView* discovery and status daemon *fvds*, and places the information into the HP OpenView database (*ovwdb*). This daemon is started by *ovstart* and is stopped by *ovstop*. To check the status of *fvovmon* use the *ovstatus* command. After *fvovmon* “discovers” a switch from *fvds,* it polls *fvds* regularly to check for status, topology, and configuration changes. To get the information from managed nodes, *fvovmon* communicates with *fvds* via a TCP port.

The following synopsis lists the various options for *fvovmon*:

> fvovmon *[-t] [-a interval] [-pdb interval] [-r interval] [-ssi interval] [-hsi interval] [-lsi interval] [-NT] [-useMgmtStatus] [-home foreview_home]*

Like *fvds*, *fvovmon* performs two kinds of updates to information in the ovwdb:

- First, it performs discovery updates, in which it polls the *fvds* for complete information about a switch, host, or link, and updates the database with the complete information. The rate at which *fvovmon* polls *fvds* about the network topology information and complete switch information is configurable using the *–a* command-line argument, or the *PollNetInterval* configuration resource.

- Second, *fvovmon* periodically updates the ovwdb with the current *status* of the devices in the network. The rate at which *fvovmon* polls *fvds* for information about the status of ATM devices is configurable for each of the following types of devices: switches, ATM-connected hosts, and links.

The following command line options are available for *fvovmon:*

–a *interval* Where *interval* is called the "polling all switches interval." It is the number of seconds *fvovmon* uses to scan all the switches discovered by fvdsd. The information about the switches, as reported by *fvds*, is added to or is updated in the database. The information includes the switch’s status, neighbors, port status, IP addresss, etc. The default polling interval is 900 seconds (15 mins).

–pdb*interval* Where *interval* is the number of seconds between subsequent complete database sweeps. *fvovmon* periodically reads each object in the OpenView database and checks if it has been updated since the last database sweep. Each object that has not been updated has its status changed to down. If the object has not been updated for one day (or a new period specified by the -r option), then *fvovmon* removes the object from the map. The database polling interval defaults to 3600 seconds (60 minutes, or 4 default polling intervals).

–r*interval* Where *interval* is called the "remove" interval and is the number of seconds that an object is allowed to remain on the map after it has become down. The default remove interval is 86400 seconds (24 hours).

–ssi*interval* Where *interval* is called the "switch status interval" and is the number of seconds that the switches’ status is polled to check for changes. The default value for the switch status interval is 30 seconds.

–hsi*interval* Where *interval* is called the "host status interval" and is the number of seconds that the hosts’ status is polled to check for changes. The default value for the host status interval is 600 seconds (10 minutes).

–lsi*interval* Where *interval* is called the "link status interval" and is the number of seconds that the links’s status is polled to check for changes. The default value for the link status interval is 300 seconds (5 minutes).

–t This option turns on tracing for *fvovmon*. The tracing output goes to a file in /usr/fore/foreview/tmp/fvovmon.log.PID.

–NT *fvovmon* is responsible for registering the workstation's IP address in the trap destination lists of managed switches, so that *fvovtrapd* receives FORE-specific traps from these switches. Specifying the –NT option prevents *fvovmon* from performing this function, thus causing *fvovtrapd* to receive no traps from managed switches.

–useMgmtStatus With this option turned on, *fvovmon* will run in the "useMgmtStatus" mode. The useMgmtStatus mode is useful in the case where specific ports, regardless of their state, need to be monitored and shown in the maps. Note that in order to run properly in this mode, *fvovmon*, *fvds*, and *fvovtrapd* all must be running in this mode. It is advisable to use the "UseMgmtStatus" resource to make sure that all daemons are running in the same mode.

Additionally, the following resources, which provide a level of redundancy to the command line options, may be set in the *ForeView* configuration file. See Chapter 3 for more information on configuration file resources.

PollNetInterval Same as option -a.

PollDBInterval Same as option -pdb.

RemoveInterval Same as option -r.

Tracing Same as option -t.

PollSwitchStatusInterval Same as option -ssi.

PollLinkStatusInterval Same as option -lsi.

PollHostStatusInterval Same as option -hsi.

ReceiveTrap If this option is off, e.g. "Fvovmon.ReceiveTrap: 0", it is equivalent to specifying -NT on the command line. If it is on, it has no equivalent command line option.

UseMgmtStatus Same as option -useMgmtStatus. Note that this option can be specified for each of the daemons, e.g. "Fvovmon.UseMgmtStatus: 1", or for all the daemons, e.g. "UseMgmtStatus: 1".

To change options for *fvovmon:*

1. Stop *fvovmon* by issuing the command **`ovstop fvovmon.`**
2. Remove the existing local registration file (lrf) bindings by issuing the command **`ovdelobj $OV_LRF/fvovmon.lrf.`**
3. Edit the lrf file to add the option flags.

For example:

```
fvovmon:/usr/OV/bin/fvovmon:
OVs_YES_START:ovwdb:-a 300:OVs_WELL_BEHAVED:15:
```

NOTE Note the placement of the option flag, “-a 300”, in the example.

4. Add back the lrf bindings by issuing **`ovaddobj $OV_LRF/fvovmon.lrf`**.
5. Restart *fvovmon* by issuing the command **`ovstart fvovmon`**.

The following are the relevant files for *fvovmon:*

$OV_LRF/fvovmon.lrf The local registration file for *fvovmon*.

/usr/fore/foreview/tmp/fvovmon.log.PID The trace file used for output from *fvovmon* with a process identification number (PID).

5.11.3 Options for Handling FORE-specific Traps

The daemon *fvovtrapd* communicates with the *ForeView* discovery and status daemon, *fvds*, to retrieve information about managed nodes. Then *fvovtrapd* updates the HP OpenView database (ovwdb) whenever it receives FORE-specific traps from managed switches. This daemon is started by *ovstart* and is stopped by *ovstop*. To check the status of *fvovtrapd,* use the *ovstatus* command.

The following command line options are available for *fvovtrapd:*

–t This option turns on tracing for *fvovtrapd.* The tracing output goes to a file in /usr/fore/foreview/tmp/fvovtrapd.log.PID.

–useMgmtStatus With this option turned on, *fvovtrapd* will run in the “useMgmtStatus” mode. Note that in order to run properly in this mode, *fvovtrapd, fvds,* and *fvovmon* all must be running in this mode. It is advisable to use the “UseMgmtStatus” resource to make sure that all daemons are running in the same mode.

The following are the relevant files for *fvovtrapd:*

$OV_LRF/fvovtrapd.lrf The local registration file for *fvovtrapd*.

/usr/fore/foreview/tmp/fvovtrapd.log.PID The trace file for output from *fvovtrapd* with a process identification number (PID).

To change options for *fvovtrapd:*

1. Stop *fvovtrapd* by issuing the command **`ovstop fvovtrapd`** .
2. Remove the existing local registration file (lrf) bindings by issuing the command **`ovdelobj $OV_LRF/fvovtrapd.lrf`** .
3. Edit the lrf file to add the option flags.

For example,

```
fvovtrapd:/usr/OV/bin/fvovtrapd:
OVs_YES_START:ovwdb:-t:OVs_WELL_BEHAVED:15:
```

NOTE Note the placement of the option flag, -t in the example.

4. Add back the lrf bindings by issuing **`ovaddobj $OV_LRF/fvovtrapd.lrf`**.
5. Restart *fvovtrapd* by issuing **`ovstart fvovtrapd`**..

5.11.4 Unmanaging Objects in the HP OpenView Database

The application *fvovunmanage*, most commonly used during installation of *ForeView*, retrieves all of the ATM objects in the HP OpenView database and sets their “ATMmon Managed” value to false. Thus, when upgrading *ForeView* to a new release, all of the ATM objects in the HP OpenView database will be re-initialized.

In addition, *fvovunmanage* also can be used interactively to unmanage specific objects in the HP OpenView database. First, the object’s database identifier must be determined. This can be done by running the *ovobjprint* command and then searching the results for the object to unmanage. The command to selectively unmanage an object is as follows:

```
fvovunmanage  [-o object_id]
```

CHAPTER 6 Running *ForeView* with SunNet Manager

This chapter provides information on how to run *ForeView* under SunNet Manager. *ForeView* includes three applications: *fvsnmdsc*, a network discovery tool; *fvsnmmon*, an ATM network monitoring tool; and *fvsnmtdl*, a daemon that maintains the trap destination lists on managed nodes in the ATM network. The discovery application, *fvsnmdsc*, contacts the *ForeView* discovery and status daemon (*fvdsd*) to retrieve the network topology and status information from the network, and places the information in the SNM database. Subsequent rediscoveries of the network update the information in the database, adding new nodes and removing old ones. The monitoring tool *fvsnmmon* may be used to monitor the properties of ATM switches in the SNM database. These applications are all tightly integrated into SNM.

6.1 Starting *ForeView* with SunNet Manager

To start *ForeView* under SunNet Manager, do the following:

- Initialize the **`.foreview`** file by providing seed switches for use in ATM network discovery
- Start the discovery and status daemon (**`fvds`**)
- Re-initialize the SunNet Manager Console
- Run the *ForeView* Discovery Tool (optional)

NOTE

The first time you start SunNet Manager, you will see a Welcome screen that provides two start-up options, HeadStart and BasicStart. Select the BasicStart option and then move on to the *ForeView* discovery.

6.1.1 Starting the Discovery and Status Daemon

ForeView utilizes a discovery and status server application that discovers *ForeRunner* switches, NNI and UNI links, and the endpoints of NNI and UNI links in an ATM network.

The discovery and status server application **`fvds`** maintains an internal cache of information that reflects the current topology and status of the ATM network. The accuracy of the information in the cache depends upon the various polling intervals given in the arguments to **`fvds`**.

NOTE

The executable **`fvdsd`** is launched by typing **`fvds`**. Users should not launch **`fvdsd`** directly.

The arguments for **`fvds`** reflect a distinction between discovery and polling. Discovery is the retrieval of a complete set of device information, including the device name, interface information, ATM (SPANS) address, device type, enclosure identifier, board number (for switch fabrics), system object identifier and all network module information, and connectivity information, including all link/port statuses, and all signalling path information (both SPANS and UNI 3.0).

Please refer to Chapter 4, Network Discovery, for information about the discovery and status server.

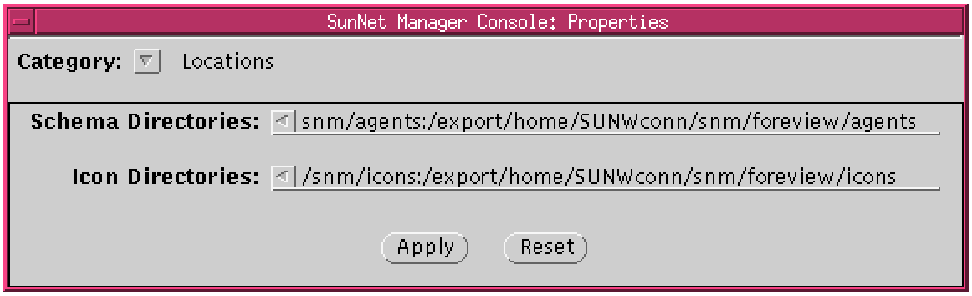
6.1.2 Initializing the SunNet Manager Database

Initialize the SunNet Manager Console by entering the following at the command line:

```
snm -i
```

This calls up the SunNet Manager Console Home View. Until the *ForeView* discovery is launched, the Home View remains empty.

If you receive an error message regarding the location of the Schema and Icon directories, you have to update the paths to these directories. You can do this from the SunNet Manager Console Properties tool. **`Apply`** the change as shown in the following figure, and re-initialize the SNM Console by re-running **`snm -i`**. Alternatively, you can edit the .**`SNMdefaults`** file from the command line before you run initially start up SNM.



SunNet Manager Console: Properties

Category: Locations

Schema Directories: snm/agents:/export/home/SUNWconn/snm/foreview/agents

Icon Directories: /snm/icons:/export/home/SUNWconn/snm/foreview/icons

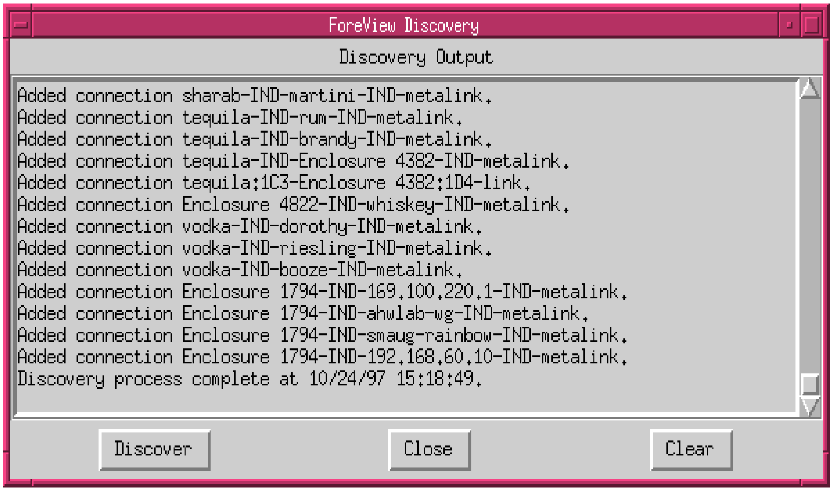
Figure 6.1 - Update Schema and Icon Directory Paths

6.1.3 Running the Discovery Tool

The **`Discovery`** tool automatically finds the elements of the ATM network and updates the SNM database. To run the Discovery tool, pull down the **`Tools`** menu from the Home View console and select **`ForeView Discovery`**. Click the **`Discover`** button on the dialog box to start the discovery.

NOTE Before running the SNM Discovery tool, make sure that the discovery and status server application **`fvds`** has completed its discovery process.

While the ATM Network is being discovered, various network components are being added to the database. Confirmation of the discovery can be viewed in the Discovery Output as shown in Figure 6.2.



```
Added connection sharab-IND-martini-IND-metalink.
Added connection tequila-IND-rum-IND-metalink.
Added connection tequila-IND-brandy-IND-metalink.
Added connection tequila-IND-Enclosure 4382-IND-metalink.
Added connection tequila:1C3-Enclosure 4382:1D4-link.
Added connection Enclosure 4822-IND-whiskey-IND-metalink.
Added connection vodka-IND-dorothy-IND-metalink.
Added connection vodka-IND-riesling-IND-metalink.
Added connection vodka-IND-booze-IND-metalink.
Added connection Enclosure 1794-IND-169.100.220.1-IND-metalink.
Added connection Enclosure 1794-IND-ahwlab-wg-IND-metalink.
Added connection Enclosure 1794-IND-smaug-rainbow-IND-metalink.
Added connection Enclosure 1794-IND-192.168.60.10-IND-metalink.
Discovery process complete at 10/24/97 15:18:49.
```

Figure 6.2 - *ForeView* Discovery Dialog

6.2 SunNet Manager's Home View

Whenever a *ForeView* session is started, the **Home** view is displayed. This is simply a symbol for the entire ATM network as shown in Figure 6.3. The color of the symbol represents the status of the ATM network.

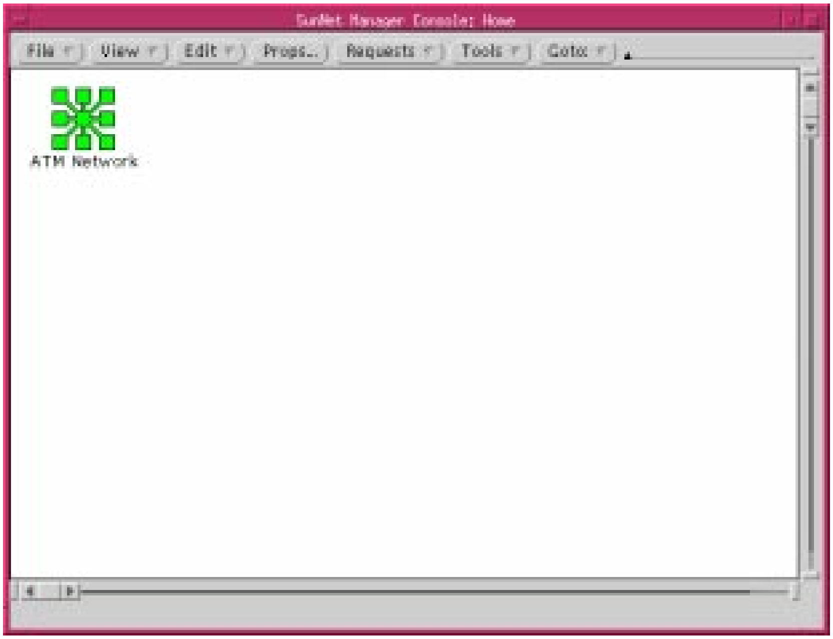


Figure 6.3 - Level 1 Home View

6.3 ATM Networks View

Double-clicking on the Home View's ATM Network glyph displays the Level 2 **ATM Network** subview. This subview displays all the nodes and the connections that exist in the managed ATM network, including:

- Switch Subnet Glyphs
- Interswitch Links

During the initial discovery of the ATM Network, the network entities are added to the subview in a clockwise pattern, starting at the top of the view. Although this layout may seem like an ordered presentation of the ATM network, it may be difficult to determine the exact nature of the interswitch connections. For ease-of-use, the glyphs in this subview may be rearranged to better illustrate the state of the interswitch connections, as shown in Figure 6.4.

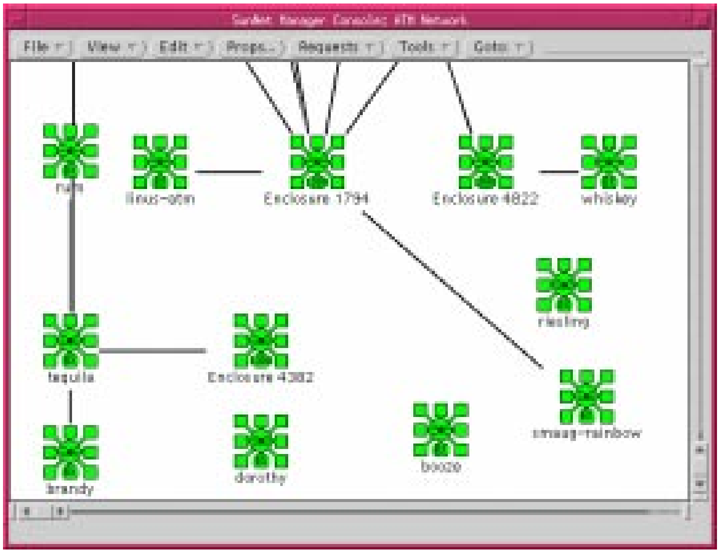


Figure 6.4 - Level 2 Subview - Arranged ATM Network Nodes

The glyphs in the ATM Network view can be arranged in any order. Subsequent runs of the **`Discover`** tool will not alter the placement of the glyphs unless the database is re-initialized.

NOTE

Glyphs located at the bottom of the ATM Network subview are switches for which no neighbors are found.

6.3.1 Interswitch Links

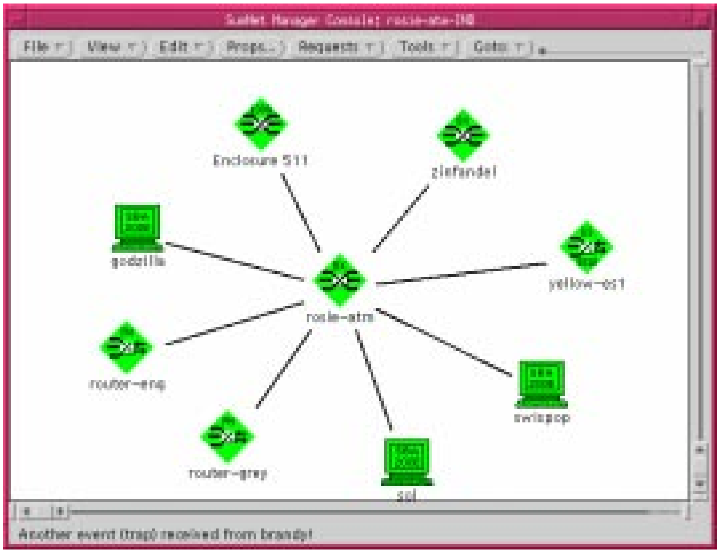
Links shown in the Level 2 ATM Network subview represent connectivity between switches in the network. Each link glyph has a subview that contains glyphs that represent the actual links in the network. Double-click on the link to bring up the subview with all individual links between the two switches.

6.3.2 Switch Subnet Glyphs

Each switch glyph in the Level 2 ATM Networks subview is labelled with the type of device; e.g., “100” means ASX-100, “200” means ASX-200, and “BX” means ASX-200BX. A glyph with a large question mark (?) in it represents a device for which the type could not be determined by the **`Discovery`**. This may be due to IP routing problems, SNMP daemon problems, etc.

6.4 Switch Connections View

Double-clicking on a switch subnet glyph in the Level 2 ATM Network subview brings up a Level 3 **Switch Connections** subview. In this subview the switch is displayed in the center of the screen and all the attached devices (hosts, switches, LAN-access devices) are displayed around it in a star layout.



Another event (trap) received from brandy!

Figure 6.5 - Level 3 Subview - Switch Connections

The connections from the center switch to its neighbors are arranged, starting at the top, in increasing order by switch port number and going clockwise. Properties of a connection, including the connection status, can be retrieved by displaying the properties dialog for the connection.

Actively monitoring the ATM Network components should be performed from the Switch Connections subview. Quick Dumps, Event and Data Requests, and other operations can be launched easily from this subview.

NOTE

Connections to ATM nodes without an IP address are not shown in *ForeView* running under SunNet Manager.

6.4.1 ATM Switch, Host, and LAN-access Device Labels

The labels of switches, hosts, and LAN-access devices such as the LAX-20 are derived from the Domain Name System (DNS). The actual name for a switch, host, or LAN Access device would be its label appended by IND (for internetworking device).

NOTE

When adding new switches or devices manually, make sure you use the correct label derived from the DNS. This is the only way SNMP queries can be performed on these devices.

For example, a switch's label on the Switch Connections view might be "cat", and if the properties were examined for that switch, the name of the switch would be "cat-IND". For *ForeRunner* ASX-1000 switches, which contain multiple switches (cluster) within a single enclosure, each enclosure has a unique enclosure id number. When a switch within a ASX-1000 enclosure is discovered, the name given to the switch has the form: **`switch-name(enclosure id)`**.

Because the enclosure id numbers may not be particularly readable, a network manager can map an enclosure id number to a string for ease of labeling. See Chapter 3 for more information on enclosure id name mapping.

NOTE

The color of the remote node indicates whether the node can be reached (pinged) from the management station, or whether a trap has been received.

6.4.2 Optional Method for Discovery

You can provide parameters to limit network discovery by providing a list of seed switches to initiate the discovery of the ATM network. The seed switches are provided in the configuration file (.**`foreview`**) using two entries. First, you must designate a list of switches, called a **`SwitchOrder`**. The discovery process discovers each switch in the **`SwitchOrder`**. Second, certain switches may be designated as seed switches by including them in the **`SeedSwitches`** entry. The discovery process uses each seed switch to find ATM neighbors to add to the SNM database.

In the simplest case, the **SwitchOrder** entry and the **SeedSwitches** entry each contain the name of one switch in the ATM network. For example:

```
SwitchOrder:      angler
SeedSwitches:     angler
```

NOTE

You need to know the name of at least one ATM switch in each ATM cloud to initiate the discovery process.

6.5 Launching *ForeView* Tools from SunNet Manager

ForeView includes several utilities which run in combination with SunNet Manager. These tools allow you to discover and monitor the ATM Network, take inventory of ATM equipment, create connections, and track network usage. You can also launch a separate ATM Network map.

Some of these tools are integrated into the pull-down **Tools** menu within the SunNet Manager Console. Others can be launched from a glyph in the Switch Connections subview. Some of these tools are available both from the pull-down **Tools** menu and from a glyph on the ATM Network or Switch Connections subviews. In addition, tools can be run outside of SunNet Manager from the command line. Please refer to the man pages in Appendix A for more information on the command line usage of these tools.

6.5.1 Activating *ForeView* Tools from the Console

Use the right mouse button to select tools from the pull-down **Tools** menu within the SunNet Manager Console. The following options are available:

ForeView Call Records... Starts the Call and Performance Records collection utilities for billing and maintenance purposes.

ForeView Config Paths/ Channels... Starts the Virtual Channel/Path tool for the creation of Paths, PVCs, and Smart PVCs. See Chapter 9 for more information about the creation of Virtual Channels.

ForeView Discover... Starts the Discovery tool which finds hosts, ATM devices, LAN-access devices, and SNMP devices reachable from the Console machine.

ForeView Inventory... Starts the Inventory utility to track devices and software in the ATM network. See Chapter 12 for more information about Inventory.

ForeView Monitor... Starts the Monitor function, which compares elements stored in the database with elements found at specified interval times.

ForeView OAM Cell Monitor... Starts the OAM (Operations and Maintenance) utility to track switch traffic problems.

ForeView RMON ST... Launches the RMON ST interface. See the *ForeView* RMON ST User's Manual for more information.

ForeView Stand-alone Map... Starts *ForeView's* Stand-alone Map. See Chapter 7 for more information on the Stand-alone Map.

ForeView Upgrade Switch SW... Starts the FORE switch software upgrade utility.

ForeView VLAN Manager Launches the VLAN Manager interface. See the *ForeView* VLAN Manager User's Manual for more information.

6.5.2 Activating *ForeView* Tools from a Glyph

To use *ForeView* tools launched from a glyph, simply select which device you want to track in the ATM Switch Connections subview. Then with the pointer over the glyph, click on the right mouse button, open the **`Tools`** menu, and select one of the menu items.

The following options are available:

NOTE When a host glyph is selected and the **`Tools`** menu is launched, only host-specific tools are available (Graph Hosts, Log Hosts).

AMI on Switch Starts an ATM Management Interface (AMI) session on the active Front Panel switch view. By default, log in as **`asx`** to access the built-in administrative tools.

Front Panel View Displays a graphical representation of an actual *ForeRunner* switch, including the number and type of network modules installed in the switch, the status of the ports on each of these modules, and the Internet name for the Ethernet Port and Control Port. See Chapter 8 for more information on the Front Panel View.

Graph Switch Ports Starts the **`Graph`** tool for selecting ports, units of measure, and parameters for selected switches or labeled links.

Graph Switch Paths Starts the **`Graph`** tool for selecting paths, units of measure, and parameters for selected switches or labeled links.

Graph Switch Channels Starts the **`Graph`** tool for selecting channels, units of measure, and parameters for selected switches or labeled links.

Graph Hosts Starts the **`Graph`** tool for selecting parameters to graph for selected hosts, labeled links, or switches.

Inventory Starts the **`Inventory`** utility. See Chapter 12 for more information on **Inventory**.

Log Switch Ports Starts the **Log** tool for selecting ports, collection intervals, and parameters for selected switches or labeled links.

Log Switch Paths Starts the **Log** tool for selecting paths, collection intervals, and parameters for selected switches or labeled links.

Log Switch Channels Starts the **Log** tool for selecting channels, collection intervals, and parameters for selected switches or labeled links.

Log Hosts Starts the **Log** tool for selecting parameters to log for selected hosts, labeled links, or switches.

Paths/Channels Config... Starts the **Virtual Channel/Path** tool for the creation of Path, PVCs, and Smart PVCs. See Chapter 8 for more information on the creation of Virtual Paths and Channels.

Trace Channels Starts the **Channel Trace** tool. See Chapter 11 for more information on Channel Trace.

Update Properties Starts the **Monitor** tool for a one-time update of a selected switch. This is useful for manually adding nodes to the network.

NOTE Please refer to Chapter 10 for more complete information on the **Graph** and **Log** tools.

6.6 ATM Network Status

The color of the ATM object (switch, host, or LAN-access device) represents its status. If a host symbol is red, that means that the host can not be reached (pinged) from the management station, or that a trap has been received.

Because the operational status is an indication of valid SPANS messages that are transmitted between the host and the switch, if the operational status is down, it indicates that either the physical link is down, or that the remote host has stopped sending SPANS messages (because it is down, or because SPANS was turned off). For more information about SPANS, refer to the *ForeRunner* ATM Switch Configuration Manual.

If the color of a switch is red, it indicates that the discovery application did not successfully poll the switch.

The color of the ATM Network symbol in the **Home** View represents the status of the entire ATM network. It is green if all switches and interswitch links in the map are OK. It will be red if any ATM switch has received a trap.

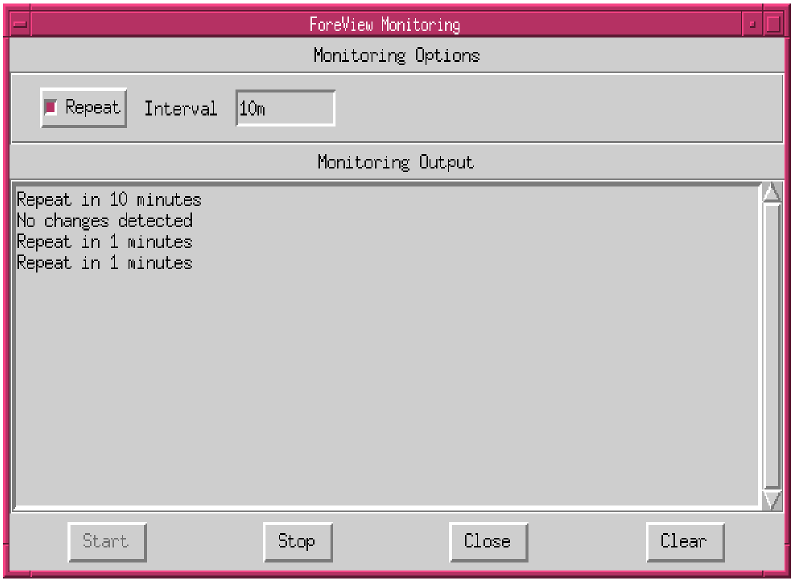
NOTE

The operational status of links between objects is not indicated by any color change in the network views.

6.7 Monitoring the ATM Network

The Discover tool function finds switches, hosts, LAN-access devices, and other Simple Network Management Protocol (SNMP) devices reachable from the network management station. On finding a network element, the discover function stores a record for that element in the SunNet Manager database.

To monitor the ATM network, pull down the **`Tools`** menu from the Home View console and select **`ForeView Monitor`**. This calls up the Monitoring Output dialog box shown in Figure 6.6.



Interval 10m

```
Repeat in 10 minutes
No changes detected
Repeat in 1 minutes
Repeat in 1 minutes
```

Figure 6.6 - Monitoring Output Dialog

The monitor function compares the properties of switches stored in the SunNet Manager database with the actual properties it retrieves from the switches in the network. An important property of each switch is its *status*. Thus, each time **`ForeView Monitor`**ing runs, it updates the database with the current status of the switches.

NOTE

The default setting for the **`ForeView Monitor`** is to repeat every 10 minutes. This setting can be modified by the network manager.

It is important to remember that **ForeView Monitor** compares only the properties of elements stored in the SunNet manager database with the properties of the elements it finds in the network at the specified polling interval. New elements are not added to the database.

NOTE

To monitor new ATM devices that were added to the network, you have to run **Discover** again.

6.7.1 SNMP Traps

A trap is an unsolicited report sent from an agent that often signifies some unexpected error condition. A *ForeRunner* switch sends traps to the network management station.

Trap reports are displayed in the **Event/Trap Reports** dialog. The report is stored in the **event.log** file and may be viewed in the **Event/Trap Reports** dialog. A list of traps is available in Appendix D.

6.7.2 Update Properties

The **Update Properties** tool, launched from a switch glyph's pop-up tool menu, is useful when manually adding nodes to the SunNet Manager database. This tool runs the **ForeView Monitor** one time for the selected switch. Simply create the glyph, provide the name and IP address values, and then run the **Update Properties** tool to fill in the remaining properties.

6.8 Re-discovering the Network

If new ATM devices were added to the network since the last discovery was run, you will want to run the **Discover** tool again. This way, the ATM Networks subview and Switch Connections subviews can be updated, and the new devices will be available for monitoring. To run the **Discovery** tool, pull down the **Tools** menu from the home View console and select **ForeView Discovery**. Click the **Discover** button on the dialog box to start the discovery.

NOTE

Glyphs representing new ATM devices are added to the bottom of the views, with the appropriate links. These glyphs can be re-positioned to present a clearer view of the internetwork connections.

The **Monitor** tool is now able to monitor the entire ATM network, including any new devices added to the network.

6.9 Troubleshooting *ForeView* on SunNet Manager

6.9.1 Problems with Discovery

The **Discovery** tool launches an executable called **fvsnmdscd**, as well as **fvsnmtdl** and **tdld**. When encountering problems with the discovery:

1. Be sure the **SeedSwitches** and **SwitchOrder** fields in the .**foreview** configuration file (Chapter 3) are correct and that the seed switches can be accessed from the network management station.
2. Run **fvsnmdscd -d 2** from the command line, and inspect the log file in **/usr/fore/foreview/tmp/fvsnmdsc.log.<pid>**.
3. Contact FORE Systems Technical Support. Refer to the Preface of this manual for more information.

6.9.2 Problems Receiving Traps

The processes **fvsnmtdl** and **tdld** manage trap destination lists on managed ATM switches in the network. One, and only one of each process, should be executing at a time. The file **/usr/fore/foreview/tmp/fvsnmtdl_running** is a “marker” file which should exist if, and only if, **fvsnmtdl** is running.

If you find that **fvsnmtdl** or **tdld** is not running, be sure that **fvsnmtdl_running** does not exist, then start the **ForeView Monitor** process. This re-starts **fvsnmtdl** and **tdld**.

6.9.3 Error Logs

Error logs exist for all *ForeView* applications. They are in **/usr/fore/foreview/tmp**. Be sure to clean out this directory periodically, especially if disk space is a concern.

CHAPTER 7 Running *ForeView's* Stand-alone Map

ForeView provides a Stand-alone network map that runs independent of a network management system. This same stand-alone map also is incorporated in *ForeView* running under the OpenWindows environment and can be launched simultaneously from *ForeView* running under OpenView, NetView or SunNet Manager. This chapter provides information on how to run the *ForeView* Stand-alone Map.

7.1 Starting the Stand-alone Map

The minimum requirements to start *ForeView's* Stand-alone Map are as follows:

- The **.foreview** file (see Chapter 3)
- For Windows NT users, the **foreview.conf** file (see Chapter 3)
- The discovery and status daemon (**fvdsd**) for network discovery

The *ForeView* stand-alone map is an application that runs on top of **fvdsd**, which collects topology and status information from the ATM network. When the stand-alone map is started, the view of the network depends on the switches specified in the resources **SeedSwitches** and **SwitchOrder** in the home directory. Refer to the configuration template file in **/usr/fore/foreview/conf** (or **$FOREVIEW_HOME/conf**) directory, to set up your .**foreview** file.

NOTE

When both the **SeedSwitches** and **SwitchOrder** in resources are not specified or when they specify no switches, the map displays all the switches and their topology discovered by **fvdsd**.

7.1.1 Limiting Network Discovery

The stand-alone map view can be limited to the switches specified in the resources **SeedSwitches** and **SwitchOrder** to initiate the discovery of the ATM network. *ForeView* retrieves the seed switches from the .**foreview** configuration file (see Chapter 3).

The seed switches are provided in the configuration file (**.foreview**) using two entries. First, you can designate a list of switches, called a **SwitchOrder**. The discovery process locates each switch in the **SwitchOrder**. Second, certain switches may be designated as seed switches by including them in the **SeedSwitches** entry. The discovery process uses each seed switch to find its ATM neighbors to add to the **fvmap** display.

In the simplest case, the **SwitchOrder** entry and the **SeedSwitches** entry each contain the name of one switch in the ATM network. For example:

```
SwitchOrder:   angler
SeedSwitches:  angler
```

NOTE

You need to know the name of at least one ATM switch in each ATM cloud in your network to initiate the discovery process.

After the file is edited and saved, run **`fvmap`** at the command line to initiate the network discovery. The default map appears, as shown in Figure 7.1. Initially, the map is empty during the discovery phase. After the discovery is complete, **`fvmap`** does periodic updates to the status of the nodes shown on the map.

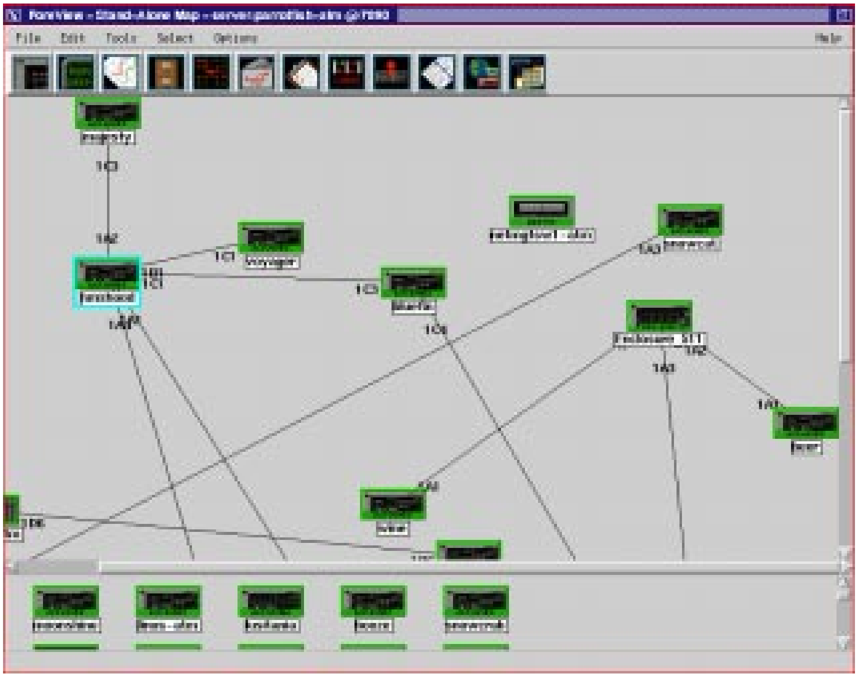


Figure 7.1 - *ForeView*'s Stand-alone Map

7.2 Viewing Options for the Stand-alone Map

When the discovery is complete, the devices (switches and LAN-access devices) are added to the map. To display all the nodes and the connections that exist for a particular switch, double click on a switch icon to view the hosts, interswitch links, and LAN-access devices for that switch.

For example, double click on the switch **hmshood** to view all the connections to that switch, as shown in the following figure. The links also include the port connections. For example, the host **oracle2.fore.com** is connected to switch **hmshood** at port 1C2; and the NNI link between **hmshood** and **bluefin** is from port 1C1 on **hmshood** to port 1C3 on **bluefin**.

Double click on **hmshood** again to close the exploded view.

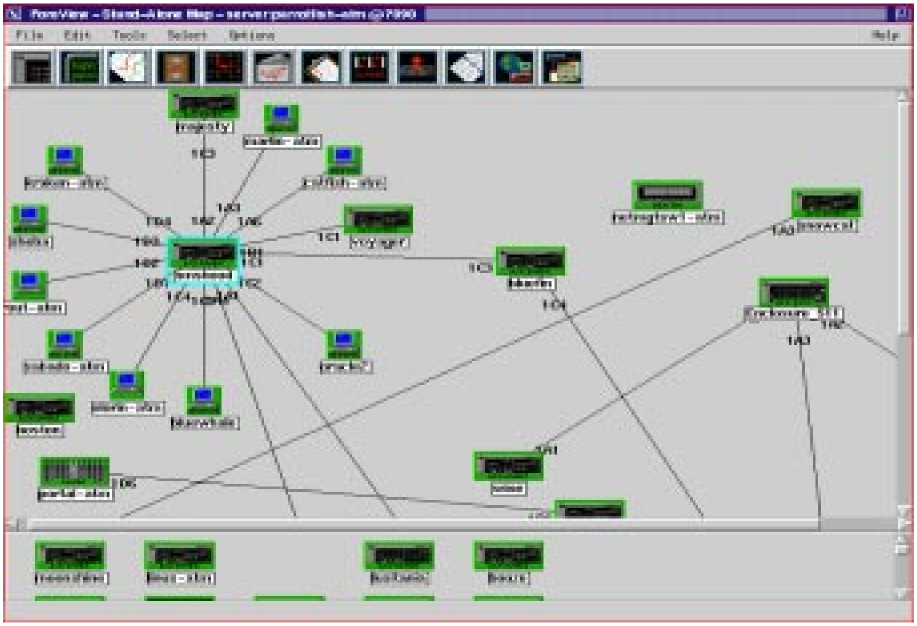


Figure 7.2 - Exploded View of a Switch

7.2.1 Launching a Connection Submap

As an alternative to viewing switch connections on the main stand-alone map, *ForeView* allows you to launch a separate connection submap for selected switches. Under the **`Options`** menu, click off the button for **`Expand SwitchView in Place`**, then double click on a switch to view all the connections to that switch on a separate map.

The following figure shows the same connections for switch **`hmshood`** as viewed in Figure 7.2, only now the connections to that switch are presented on a separate map. Pull down the **`File`** menu and select **`Exit`** to close the connection map.

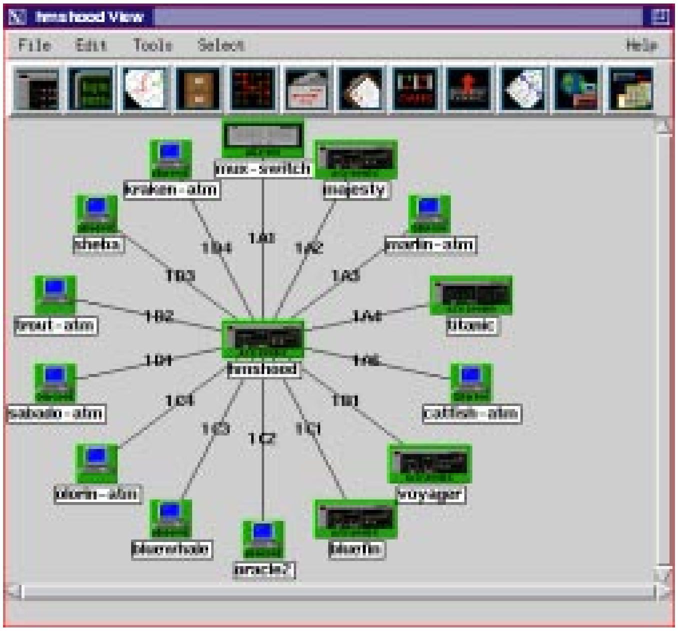


Figure 7.3 - Connection View of a Switch

NOTE Icons in the map also provide labels indicating the type of *ForeRunner* ATM device (ASX switches or ATM adapter cards).

7.3 Menus

The menu bar at the top of the map provides the following controls and commands:

7.3.1 File

The **`File`** option determines which group/sets of switches/nodes appear on the map. The following options are available:

default Shows all the switches connected to the seed switch given in **`.foreview`** (**`foreview.conf`** for Windows NT). This is not necessarily the complete ATM network layout.

Print... Allows the map layout to be printed to a file or to a postscript printer.

Exit Closes the Stand-alone map.

7.3.2 Edit

The **`Edit`** option allows you to select a switch on the map. The following options are available:

Find Allows searches for individual switches, hosts, and devices based on labels or IP addresses.

Find Next Allows searches for multiple matches to a device label or IP address string.

7.3.3 Tools

ForeView includes several utilities. These tools allow you to monitor selected ATM switches, links, and hosts. Tools are available from the pull-down **`Tools`** menu, or from the Toolbar directly under the menus. The following options are available:

Front Panel Provides a graphical representation of an actual *ForeRunner* switch, including the number and type of network modules installed in the switch, the status of the ports on each of these modules, and the Internet name for the Ethernet Port and Control Port.

Allows you to monitor network links and devices and provides detailed views of FORE Systems' LAN-access products on the network, including the LAX-20, PowerHubs, ES-3810, and ES-3850.

AMI Starts an ATM Management Interface (AMI) session on a selected switch. By default, log in as **asx** to access the built-in administrative tools.

Graph Select one of the four menu items: switch ports, switch paths, switch channels, or hosts. This method works for graphing network usage for switches, links, and hosts in your network. See Chapter 10 for more information on Graphing.

Log Select one of the four menu items: switch ports, switch paths, switch channels, or hosts. This method works for logging network usage for switches, links, and hosts in your network. See Chapter 10 for more information on Logging.

Config Paths/Channels Launches the **Virtual Channel/Path** tool for the creation of Paths, PVCs, Smart PVCs, and Signalling Paths. See Chapter 9 for more information on the creation of Virtual Channels.

Trace Paths / Channels Launches the **Channel/Path Trace** tool. See Chapter 11 for more information on Channel Trace.

Inventory Launches the **Inventory** utility. See Chapter 12 for more information on **Inventory**.

Upgrade Switch Launches the switch software upgrade utility.

Call Record Launches the call and performance record collection utility, useful for billing and maintenance information. See Chapter 14 for more information on Call Records.

OAM Monitor Launches the OAM Monitor window, which is used for troubleshooting traffic problems. See Chapter 13 for more information on the OAM feature.

VLAN Manager Launches the VLAN Manager interface. See the *ForeView* VLAN Manager User's Manual for more information.

ForeView RMON ST Launches the RMON ST interface. See the *ForeView* RMON ST User's Manual for more information.

7.3.4 Select

This option provides selection options that are useful when running some of the utilities found under **`Tools`**. The following options are available:

Switches Selects only switches on the map.

Hosts Selects only hosts on the map.

Devices Selects from FORE devices on the map such as the CellPath 90/90E, CellPath 300, ES-3810, ES-3850, The LAX-20, and PowerHubs.

7.3.5 Options

This menu provides control for the switch connection view. When selecting devices for monitoring, two view modes are provided for the connection layout. The following preferences are available:

Expand SwitchView in Place When **`Expand SwitchView in Place`** is on, selected switches showing all attached nodes, including hosts, switches, and devices, are displayed on the main stand-alone map.

When **`Expand SwitchView in Place`** is off, selected switches showing all attached nodes, including hosts, switches, and devices, are displayed on separate maps.

Polling Establishes a polling interval for the displayed switches, hosts and links. Polling can be set to 1, 5 or 10 minute intervals. Polling also can be turned off entirely or it can be on demand.

7.3.6 Help

Brings up the on-line help utility.

7.4 Navigating the Map

It is helpful to remember the following points when navigating the *ForeView* Stand-alone map.

- Double-clicking on a switch icon explodes the view to show connected nodes. Double-clicking on the same switch icon closes the exploded view.
- Customized views can be created to provide distinct view of network work groups, such as software, engineering, or accounting.
- Tools are available from either the pull-down **`Tools`** menu, or from the Toolbar directly under the menus.
- Switch connections can be displayed either on the main map or on a separate map using the **`Expand SwitchView in Place`** option.

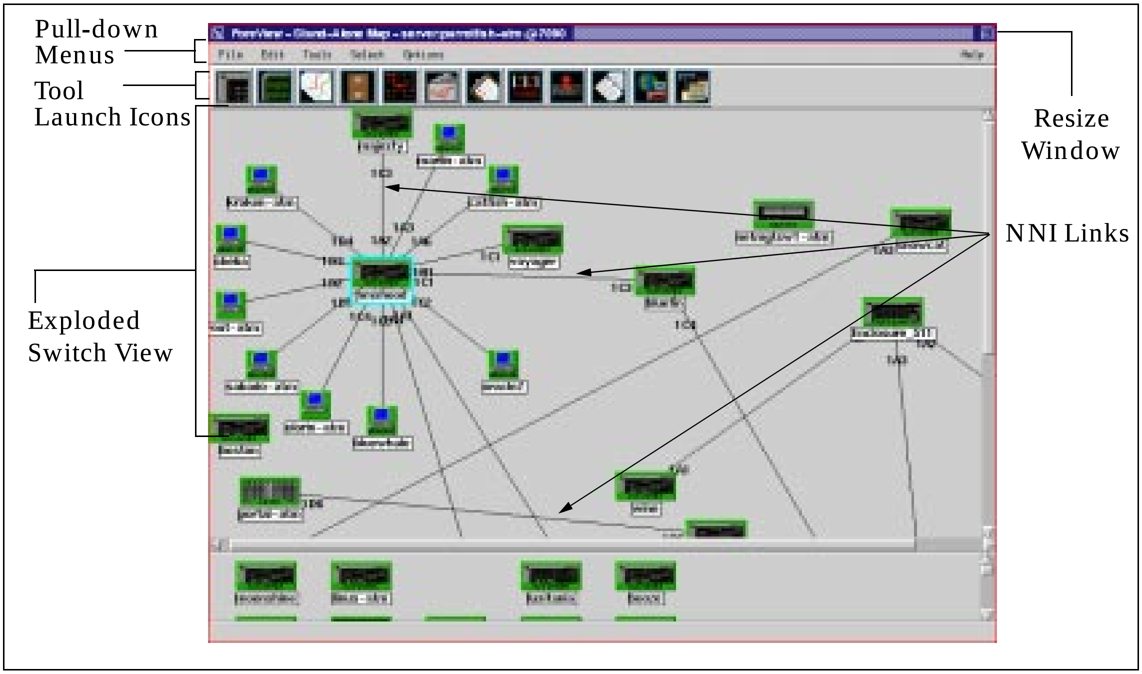


Figure 7.4 - Elements of the Stand-alone Map

CHAPTER 8 Front Panel

The Front Panel option allows you to view a graphical representation of an actual ATM switch, including the number and type of network modules installed in the switch, the status of the ports on each of these modules, and the Internet name for the Ethernet Port and Control Port.

The graphical representation of the network modules also shows the name of the workstation connected to each port, a tachometer icon which can be selected to show the instantaneous throughput of a given port, as well as port gauges which illustrate bandwidth allocation and queue loading.

To access a Front Panel for an ATM switch, select (single click) one or more switch icons in the ATM Map (either diamond or circle symbols), pull down the *ForeView* menu item, and choose Front Panel. Version 4.3 of *ForeView* supports the ASX-1000, ASX-200BX, ASX-200WG, and the ASX-200 ATM switches, as well as TNX switches for service providers. In addition, the Front Panel can be launched against FORE Systems' LAN-access products on the network, including PowerHubs, CellPaths, and ES-3810s.

The switch control software includes an SNMP agent that enables the remote monitoring and configuration of FORE switches. Please refer to the table in Appendix B for a summary of the port number conventions used in FORE switches and related SNMP indexing format.

8.1 ATM Backbone Switches

The *ForeRunner* ASX-1000, the ASX-200BX, and the MSC-900 switches are designed specifically to meet the needs of LAN backbone networks.

8.1.1 ASX-1000

The ASX-1000, as shown in Figure 8.1, is a self-contained ATM switch that provides an Ethernet connection for network management access. The hardware for the ASX-1000 consists of up to four switch boards, each with an i960 SCP; network modules; redundant power supplies; a Common Equipment Card (CEC); and a removable fan tray. These components work together to provide ATM switching capabilities, as well as distributed connection setup and management.

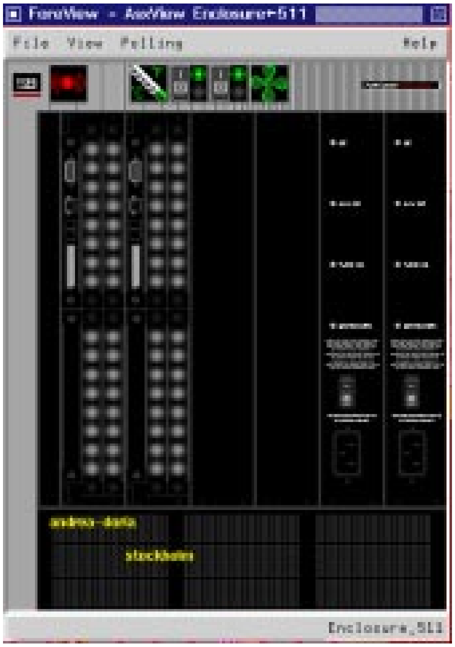


Figure 8.1 - The Front Panel of the ASX-1000

8.1.2 ASX-200BX

The ASX-200BX, as shown in Figure 8.2, is a self-contained ATM switch that provides an Ethernet connection for network management access. The ASX-200BX hardware consists of a single switch board with an i960 SCP, network modules, redundant power supplies, and fans. These components work together to provide ATM switching capabilities, as well as distributed connection setup and management. The ASX-200BX provides connectivity for up to 16 computer workstations, hubs, or routers at rates operating up to 155 Mbps/sec (or 24 workstations running at 100 Mbps) via dedicated fiber optic links and twisted pair links.

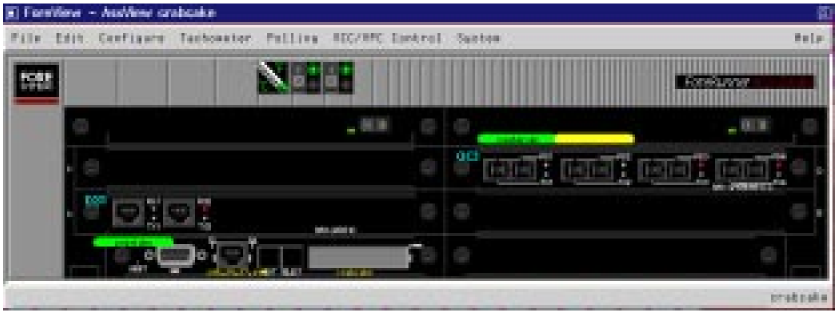


Figure 8.2 - The Front Panel of the ASX-200BX

8.1.3 MSC-900

The MSC-900 acts as a stand-alone low-speed port concentrator designed to conduct low-speed ports (J-2, E-1, DS-1, E-3, and DS-3) into high-speed ATM uplinks. The hardware for the MSC-900 consists of up to four switch boards, each with an i960 SCP; network modules; redundant power supplies; a Common Equipment Card (CEC); and a removable fan tray. These components work together to provide ATM switching capabilities, as well as distributed connection setup and management.

Wide-area network (WAN) connectivity is seamlessly integrated into the ASX-1000, the ASX-200BX, and the MSC-900 switches for connection to private networks or ATM services via OC-3/OC-12 (SONET), DS-1, DS-3, E-1, E-3, J-2, or TP-25 network modules.

8.1.4 TNX-210

The TNX-210 uses a unique 2.5 Gbps switch fabric. The standard TNX-210 configuration consists of a chassis, a 2.5 Gbps switch fabric, four network module slots, dual i960-HA32 SCPs, dual power supplies (AC or DC), and *ForeThought* service provider software. In addition to supporting a full range of ATM modules, the TNX switches support circuit emulation network modules for providing TDM (Time Division Multiplexed) services similar to those provisioned using 0-1 DCS (Cross-Connect Systems).

8.1.5 TNX-1100

The TNX-1100 is a modular system consisting of a chassis configured with redundant common system modules including AC or DC power supplies, CEC-Plus modules and switch control processors for each switch fabric. The standard TNX-1100 configuration consists of a chassis, (1-4) 2.5 Gbps switch fabrics, four network module slots per switch fabric, dual i960-HA32 SCPs per switch fabric, the CEC-Plus, dual power supplies (AC or 30A-DC), and *ForeThought* service provider software.

The TNX-1100 system architecture is based on FORE’s award-winning distributed switch design supporting in-service system upgrades from 2.5 Gbps to 10 Gbps switching capacity.

- Scalable, non-blocking ATM switch
- In-service switch expansion from 2.5 to 10 Gbps
- 4-16 network module slots
- Redundant switch control processors
- Redundant AC and DC power, fans
- Hot swappable fabrics, processors, power supplies, fans, clock and network modules

8.2 ATM Workgroup Switches

The *ForeRunner* ASX-200WG and the ASX-200 ATM switches are designed to bring high performance ATM connectivity to LAN workgroup applications.

The ASX-200WG, as shown in Figure 8.3, is a self-contained ATM switch that provides an Ethernet connection for network management access. The ASX-200WG ATM switch hardware consists of a single switch board with an i960 SCP, network modules, and fans. These components work together to provide ATM switching capabilities, as well as distributed connection setup and management.

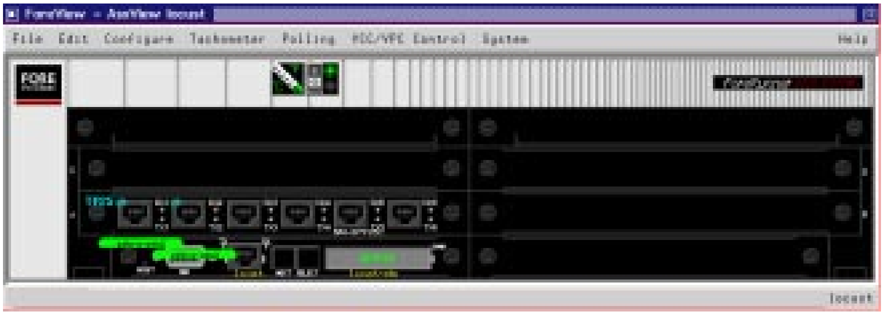


Figure 8.3 - The Front Panel of the ASX-200WG

The ASX-200, as shown in Figure 8.4, is a self-contained ATM switch that provides an Ethernet connection for network management access. The ASX-200 hardware consists of a single switch board, a SPARC RISC switch control processor (SCP), network modules, and fans housed in a rack-mount 19-inch horizontal enclosure. These components work together to provide ATM switching capabilities, as well as distributed connection setup and management.

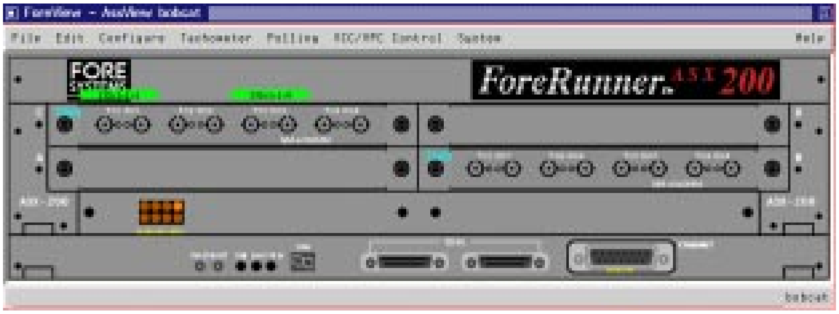


Figure 8.4 - The Front Panel of the ASX-200

8.3 Switch Control Processors

The SPARC RISC SCP in the ASX-200 and the i960 SCP in the ASX-200WG, ASX-200BX, and the ASX-1000 provide the distributed connection setup for a network of ATM switches. The SCP primarily provides management access through SNMP and is responsible for storing and updating all SNMP management information. Additionally, the SCP has direct access to the switch board. The SCP, and associated software, manages the behavior of the switch board (i.e., connection setup), but is not involved in the actual cell switching.

8.3.1 SPARC RISC Switch Control Processor

The front panel of the ASX-200's SPARC RISC SCP includes a RESET switch; an ABORT switch; three single LEDs: the RUN / RESET LED, the VME BM (Bus Master) LED, and the STATUS LED; a diagnostics display; two serial ports (labeled A and B); and an Ethernet port.

8.3.2 i960 Switch Control Processor

The front panel of an i960 SCP for the ASX-200WG, ASX-200BX, and the ASX-1000 includes the following features: a RESET button, an RS-232 serial port, an Ethernet 10BaseT port, a NEXT pushbutton, a SELECT pushbutton, a display LED, and a power LED.

NOTE

After the boot process and self-diagnostics are complete, the name of the SCP is shown in the display LED during normal operations, if an SCP name has been assigned. If an SCP name has not been assigned, it will display `ATM SWITCH`.

Front Panel

8.4 Network Modules

The *ForeRunner* LAN and WAN network modules are the physical ATM port interface cards that provide LAN/WAN connectivity to other ATM switches, ATM-compatible desktop computers and servers, hubs, routers, multiplexers, and carrier ATM services. Currently, network modules are available to provide ATM connections ranging from 1.5 Mbps to 622 Mbps over both fiber-optic and copper media.

The network modules in a *ForeRunner* switch board act as the physical input/output ports to the switch board. A network module may have one, two, four, or six physical ports, depending on its configuration.

8.4.1 Port Numbering

The individual ports on a network module are numbered according to the Board-Network Module-Port (BNP) notation.

Board Refers to the number of the switch board that contains the port being numbered. “Board” is always 1 in an ASX-200, ASX-200BX, or an ASX-200WG, since these switches each contain only one switch board. “Board” can be 1, 2, 3, or 4 in an ASX-1000, depending on the number of the physical switch board that contains the port being numbered.

Network Module Refers to the slot (A, B, C, or D) in the switch board that contains the port being numbered.

Port Refers to the physical port (1 - 6) being numbered on the individual network module.

For example, according to this notation, the fourth port on a network module in slot B of switch board #2 is port 2B4.

8.5 Port Indicators

There are status and information indicators on each port icon. Depending on the type of network module installed, some ports appear slightly different than the illustration below.

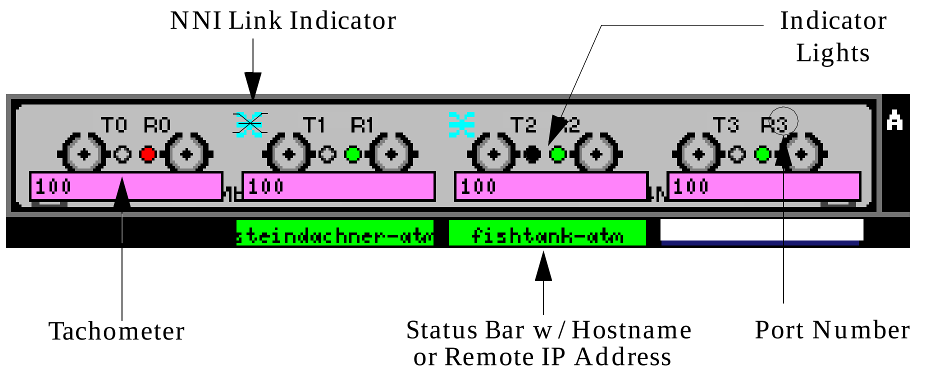


Figure 8.5 - Port Indicators

Status Bar The status bar displays the hostname or IP address of the SPANS interface. By default, the IP address is displayed.

The color of the status bar indicates the status of SPANS. A **green** status bar indicates SPANS is enabled and up on that port. **Yellow** indicates SPANS is enabled, but down, on that port. No status bar means there is no carrier on the port (see Indicator Lights). Ports that are yellow can indicate a remote device that is in the process of booting. Yellow ports also can be a result of SPANS being down and UNI signalling being up. If the port remains yellow, administrative action is probably required.

NNI Link Indicator The link indicator identifies a network-to-network interswitch (NNI) connection, showing that the port is attached to another *ForeRunner* switch.

Port Number (NP) The port number uniquely identifies the port throughout the switch and is used to refer to the port during management tasks. It is derived from the NP notation that includes the network module identifier (A-D) plus the actual port number.

Indicator Lights The indicator lights show the state of the physical connection on the port. The **Rx** is the carrier light. It is green when the port detects a carrier and it is red otherwise. The **Tx** shows line error indications. The line error indicator typically is the same color as the port itself; if there are line errors, it turns yellow. The line indicator is also yellow if it has been administratively forced up and a carrier is not present.

Tachometer The tachometer shows the level of activity on a given port. The **`Tachometer`** menu is used to select the type of activity shown. The number in the tachometer shows the value of the chosen parameter in percent, the colored bar is a semi-logarithmic representation of the percentage.

8.6 Menu Bar

The menu bar at the top of the switch image provides the following controls and commands:

8.6.1 File

File / AMI on switch... Starts an ATM Management Interface (AMI) session on the active Front Panel switch view. By default, log in as **`asx`** to access the built-in administrative tools.

File / View Remote... Starts a front panel session with a remote switch connection. To launch the remote front panel, select a port with an NNI link indicator and click on the **`View Remote...`** option.

File / Quit Closes the Front Panel application.

8.6.2 Edit

Use the **`Edit`** menu to select media-specific ports. Options are:

Edit /Select all ports Selects all network module ports on a Front Panel.

Edit /Select all DS1 ... TP25 Ports Selects any available port on a Front Panel, including DS-1, DS-3, E-1, E-3, J-2, OC-3, OC-12, TAXI-100, TAXI-140, TP-25, CEMDS1, and CEME1 ports.

Edit /Clear selection Clears any ports currently selected on a Front Panel.

8.6.3 Configure

Use the **`Configure`** menu to configure ports (either individual or multiple) and network modules. See sections 8.8 through 8.13 provide more detailed explanations of these menu options.

Configure /Port Configures a port or multiple ports selected from a Front Panel. Ports can be selected using the Edit pull down menu. Options for this menu item are Generic, LED Mode, OC3/OC12, DS3, DS1, E3, E1, J2, TP25, CEMDS1, CEME1, Traffic, CAC, and Port/OAM Admin. Also, you can right-click on a port to bring a pop-up menu for that port.

Configure /Module Configures a network module. Options for this menu item are Traffic, which makes use of network module shared memory. Series C and Series LC network modules are the only modules that have shared memory.

Configure/Timing Configures or displays information about the timing source of the network modules.

Configure /IP Configures remote IP Interfaces and Routes.

Configure /Signalling Provides port signalling control and monitoring for SPANS and UNI 3.x signalling. Also provides the means to create signalling paths.

Configure /Alarms This menu allows you to view the state of and change the priority of alarm types related to ASX-1000, ASX-200WG. ASX-200BX and ASX-200BXE switches.

Configure /NSAP Configures NSAP prefixes and addresses.

Configure/Models Configures memory models for shared memory network modules. Series C and Series LC network modules are the only modules that have shared memory.

Configure /UPC Configures Usage Parameter Control (UPC) contracts that establish Quality of Service on VCCs. See Chapter 9.

Configure /AVR Configures the Address Validation threshold.

Configure /PMP Configures the Point-to-Multipoint minimum and maximum VCI allocation.

Configure /PNNI-SPVC Configures Pacing and Rerouting parameters for the PNNI SPVCs.

8.6.4 Tachometers

The tachometer shows the level of activity on a given port. The number in the tachometer shows the value of the chosen parameter in percent, the colored bar is a semi-logarithmic representation of the percentage.

The **`Tachometer`** menu allows you to select the type of information that is displayed within the per port tachometers. These are:

None Tachometer not selected.

Input Utilization The portion of the port's input capacity that is currently being used. For example, if a port capable of handling an input of 155 megabits per second is currently receiving 116 megabits per second, the tachometer will show 75% utilization.

Output Utilization The portion of the port's output capacity that is currently being used.

Input Reservation The portion of the port's input capacity that has been reserved for use by all of its virtual circuits.

Output Reservation The portion of the port's output capacity that has been reserved for use by all of its virtual circuits.

Output Queue Loading The portion of the port's output buffer that is currently full. This tachometer will typically show little or no activity; values approaching 100 would indicate incipient link overloading.

Absolute Values Shows bytes/sec instead of percentage loads.

8.6.5 Polling

The Front Panel will periodically poll the switch for status updates. The polling interval can be changed by using the **`Polling`** menu. The default polling interval is every thirty seconds, but can be changed to 10 or 60 seconds. Polling can also be turned off through the same menu.

As long as a polling interval of any duration is selected, the orange switch lights will blink once a second. When a poll is in progress, the message **`Polling`**... will appear in the lower left corner of the *ForeView* window.

If the switch fails to respond to a status query, the entire switch picture will be washed with a red overlay and a dialog box reporting the cause of the error will pop up. Choosing **`Retry`** from the dialog box will retry the attempt to contact the switch; choosing **`Quit`** will give up and close the application.

Polling / No Polling The **`No Polling`** menu entry will not poll the switch's status.

Polling / 10 Seconds The **`10 Seconds`** menu entry will set the poll of a Front Panel switch to every 10 seconds.

Polling / 30 Seconds The **`30 Seconds`** menu entry will set the poll of a Front Panel switch to every 30 seconds.

Polling / 60 Seconds The **`60 Seconds`** menu entry will set the poll of a Front Panel switch to every 60 seconds.

Polling / Demand Poll The **`Demand Poll`** menu entry will immediately force a poll of the switch's status, regardless of what the polling interval is set to.

8.6.6 VCC/VPC Control

The following menu items provide information on connections. Refer to Chapter 9 for detailed information about connections and the use of the Channel Tool.

VCC/VPC Control / PVC Starts the Channel Tool for viewing, creating, and changing Permanent Virtual Circuits.

VCC/VPC Control / Smart PVC Starts the Channel Tool for viewing, creating, and changing Smart PVCs between two end points.

VCC/VPC Control / PVP Starts the Channel Tool for viewing, creating, and changing incoming Permanent Virtual Paths.

SigPath Starts the Channel Tool for viewing, creating, and changing signalling paths, including SPANS and UNI 3.x signalling paths.

PNNISPVC Starts the Channel Tool for viewing, creating, and changing PNNI Smart PVCs.

Path Starts the Channel Tool for viewing, creating, and changing an incoming path for PVCs.

OPath Starts the Channel Tool for viewing, creating, and changing an outgoing path for PVCs.

VCC/VPC Control / Trace VC/VP Starts the Channel Trace tool. See Chapter 11 for information on Channel Trace.

8.6.7 System

The **`System`** menu allows you to view information about a switch and provides access to the OAM F4/F5 Cell Monitor. The menu items are:

Information Provides information about the switch, including uptime, software and hardware versions.

OAM F4/F5 Cell Monitor Launches the OAM Monitor window, which is used for troubleshooting traffic problems.

8.6.8 Help

Provides on-line help for Front Panel on a variety of subjects.

8.7 Configuring and Monitoring Ports

By selecting a port from a Front Panel, you can access several submenus that allow you to configure the port or monitor port statistics. You can select one port or multiple ports.

The **`Configure /Port`** option of the Front Panel provides the following choices:

Generic This menu allows you to select any port, regardless of type, and view statistics and create signalling paths. The Media Specific option provides access to the port control options when the specific media is recognized as OC3/OC12, DS3, DS1, E3, E1, or J2.

OC3/OC12 This menu allows you to select any OC-3 or OC-12 port and change control options, view statistics and create signalling paths.

DS3 This menu allows you to select any DS-3 port and change control options, view statistics and create signalling paths.

DS1 This menu allows you to select any DS-1 port and change control options, view statistics and create signalling paths.

E3 This menu allows you to select any E-3 port and change control options, view statistics and create signalling paths.

E1 This menu allows you to select any E-1 port and change control options, view statistics and create signalling paths.

J2 This menu allows you to select any J-2 port and change control options, view statistics and create signalling paths.

TP25 This menu allows you to select any TP25 port and change control options, view statistics and create signalling paths.

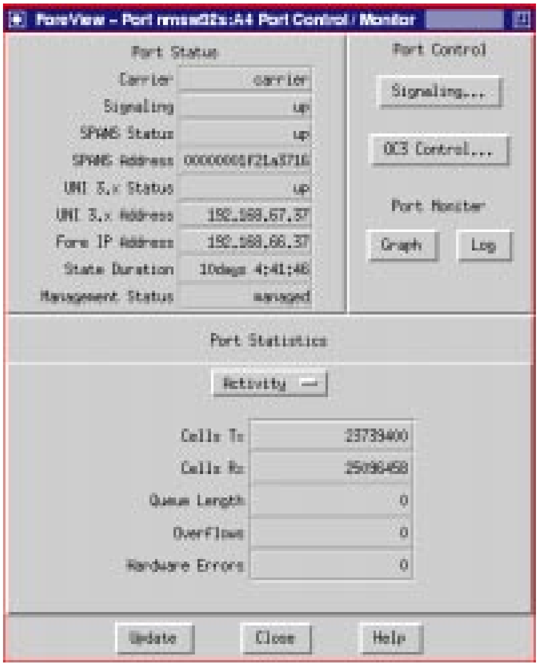
Traffic This menu allows you to configure port-specific network module shared memory options.

CAC This menu allows you to configure overbooking parameters for VBR traffic.

Port/OAM Admin This menu allows you to enable the generation of OAM cells.

8.8 Generic Port Configuration

Selecting a port/module and then launching **`Configure/Port/Generic`** from a front panel calls up the Control/Monitor dialog for generic port types. From this dialog configure the port signalling, check the port status, view port statistics, and launch a media-specific dialog.



Carrier: carrier
Signaling: up
SPANS Status: up
SPANS Address: 00000001f21a5716
UNI 3.x Status: up
UNI 3.x Address: 192.168.67.37
Fore IP Address: 192.168.66.37
State Duration: 10days 4:41:46
Management Status: managed

Cells Tx: 23739400
Cells Rx: 25096458
Queue Length: 0
Overflows: 0
Hardware Errors: 0

Figure 8.6 - Generic Port Configuration Dialog

The fields of this dialog are defined as follows:

8.8.1 Port Status

Carrier Shows whether or not a carrier has been detected on the port. If a carrier has been detected, the word **`carrier`** is displayed. If a carrier has not been detected, the word **`noCarrier`** is displayed. A carrier is detected when a signal is applied to the receive side of the port. It does not guarantee that the signal is the proper frequency.

Signalling Reflects the status of UNI signalling as either up or down.

SPANS Status Reflects the status of SPANS as either up or down.

SPANS Address Shows the SPANS address of remote interface.

UNI 3.x Status If UNI 3.x signalling is enabled, shows the status of this signalling.

UNI 3.x Address If UNI 3.x signalling is enabled, shows the address of the remote interface.

FORE IP Address Shows the IP address of FORE IP interfaces.

State Duration Displays the amount of time the port has remained up.

Management Status Displays the status of the port, either managed or unmanaged.

8.8.2 Port Control

Signalling Launches the signalling configuration dialog, also found under the Configure pull down menu.

Media Specific Control... Identifies the type of network module. If unknown, this is disabled. If the port can be identified, such as DS-3, OC-3, etc., then port control options can be launched from here.

Port Monitor (Graph and Log) Launches the graphing and logging utilities for the selected port.

8.8.3 Port Statistics--Activity

Select **`Activity`** from the Port Statistics pull-down menu to view the following statistics:

Cells Tx Displays the number of non-null ATM cells that were transmitted.

Cells Rx Indicates the number of ATM cells that were received.

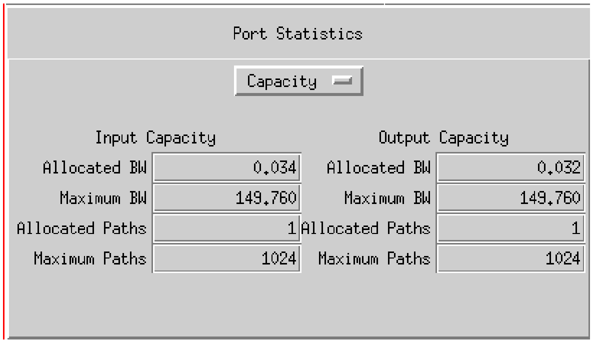
Queue Length Lists the number of cells currently in this queue.

Overflows Indicates the number of overflows in this queue.

Hardware Errors For TAXI network modules and for DS-3 Series A network modules, lists the number of Header Check Sequence (HCS) errors or physical framing errors. For all other network modules, lists the number of HCS errors.

8.8.4 Port Statistics--Capacity

Select **`Capacity`** from the Port Statistics pull-down menu to view the following statistics:



Port Statistics

Capacity

Input Capacity		Output Capacity	
Allocated BW	0.034	Allocated BW	0.032
Maximum BW	149.760	Maximum BW	149.760
Allocated Paths	1	Allocated Paths	1
Maximum Paths	1024	Maximum Paths	1024

Figure 8.7 - Port Statistics (Capacity) Dialog

8.8.4.1 Port Statistics--Input Capacity

Allocated BW Shows the amount of bandwidth (in megabits/second) that has been reserved on the port for the input link on the port.

Maximum BW Indicates the peak bandwidth rate at which the channel is policed.

Allocated Paths Designates the number of Virtual Paths that have been established on the port for the input link on the port.

Maximum Paths Designates the maximum number of Virtual Paths available on the port for the input link.

8.8.4.2 Port Statistics--Output Capacity

Allocated BW Shows the amount of bandwidth (in megabits/second) that has been reserved on the port for the output link on the port.

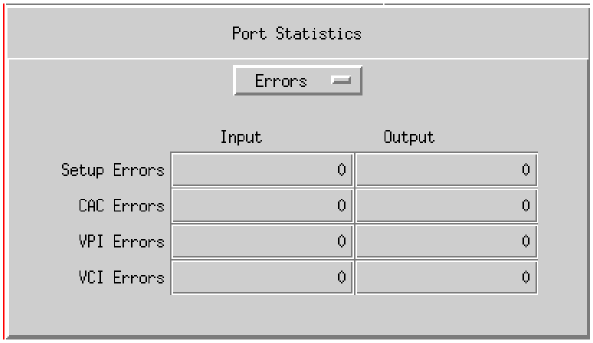
Maximum BW Indicates the amount of maximum bandwidth available.

Allocated Paths Designates the number of Virtual Paths that have been established on the port for the output link on the port.

Maximum Paths Displays the maximum number of paths available on the port.

8.8.5 Port Statistics--Errors

Select **`Errors`** from the Port Statistics pull-down menu to view the following statistics:



Port Statistics

Errors

	Input	Output
Setup Errors	0	0
CAC Errors	0	0
VPI Errors	0	0
VCI Errors	0	0

Figure 8.8 - Port Statistics (Capacity) Dialog

Setup Errors The number of input (or output) connection setup failures on this port that occur if the connection cannot be set up on the fabric because the output (or input) network module cannot support the connection for various reasons, or because a connection ID cannot be allocated on an ASX-1000 fabric.

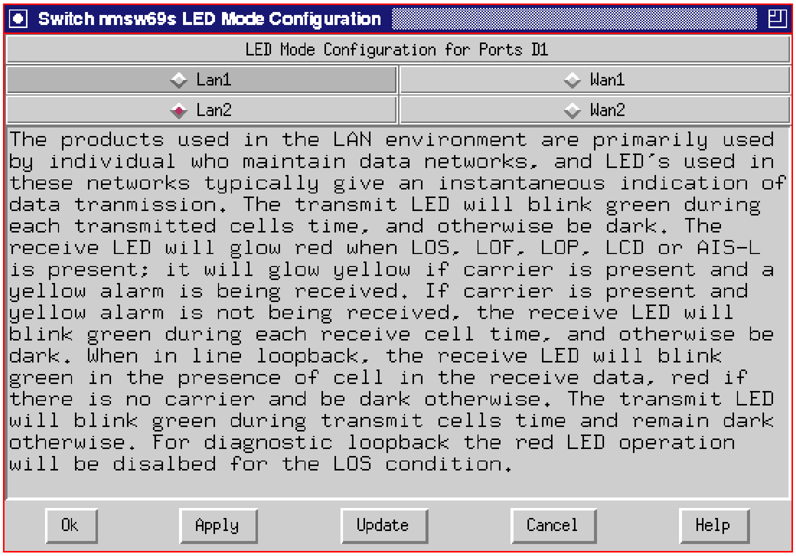
CAC Errors The number of input/output CAC failures on this port. These failures occur when there is not enough input/output bandwidth on the link or on an input/output path of that link for a connection.

VPI Errors The number of input/output VPI allocation failures on this port that occur when an input/output VPI cannot be allocated because the VPI is already in use, because the VPI is out of range, or because no more VPIs are available for allocation.

VCI Errors The number of input/output VCI allocation failures on this port that occur when an input/output VCI cannot be allocated on a path because the VCI is already in use, because the VCI is out of range, or because no more VCIs are available for allocation on the input/output path.

8.9 LED Mode Port Configuration

This option let you configure a model for the front panel LEDs on a Series C or a Series LC SONET (OC-3 and OC-12) network module. To configure, check the status of, and view the LED model for OC-3 and OC-12 ports, select the OC-3 or OC-12 port(s) from a front panel, pull down the **`Configure/Port`** menu, and launch the **`LED Mode`** dialog. The **`LED Mode`** dialog is shown in the following figure:



LED Mode Configuration for Ports D1

○ Lan1 ○ Wan1
● Lan2 ○ Wan2

The products used in the LAN environment are primarily used by individual who maintain data networks, and LED's used in these networks typically give an instantaneous indication of data tranmission. The transmit LED will blink green during each transmitted cells time, and otherwise be dark. The receive LED will glow red when LOS, LOF, LOP, LCD or AIS-L is present; it will glow yellow if carrier is present and a yellow alarm is being received. If carrier is present and yellow alarm is not being received, the receive LED will blink green during each receive cell time, and otherwise be dark. When in line loopback, the receive LED will blink green in the presence of cell in the receive data, red if there is no carrier and be dark otherwise. The transmit LED will blink green during transmit cells time and remain dark otherwise. For diagnostic loopback the red LED operation will be disalbed for the LOS condition.

Figure 8.9 - Port LED Mode Configuration Dialog

This dialog lets you select an LED model to use for setting the LED colors on a per-port basis on a SONET Series C or Series LC network module. Typically, the LAN LEDs blink when transmitting or receiving data on a port. Typically, the WAN LEDs illuminate solid green, unless an error condition exists on a port. Select one of the following parameters:

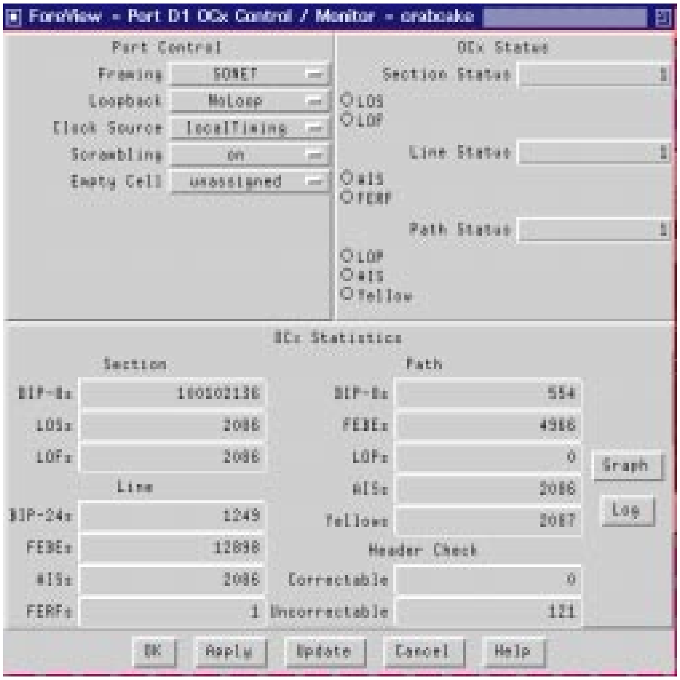
Lan1 or Wan1 For these models, RED means a fault in the receive direction, YELLOW means a fault in the transmit direction (Line Remote Defect Indication), AUTO/GREEN means no fault. Only the receive LED color is changed. These models show only three states and do not reflect the status of the Path Alarm Indications and Path Remote Defect Indications. `lan1` is the default value for all network modules.

Lan2 or Wan2 For these models, RED means a line fault, YELLOW means a path fault, and AUTO/GREEN means no fault. The transmit LED shows faults in the transmit direction and the receive LED shows faults in the receive direction. These models provide a unique LED color pattern for all six fault states that can be detected by SONET signalling.

NOTE For the Lan 2 and Wan 2 models, faults in the receive direction may make it impossible to detect certain faults in the transmit direction.

8.10 Configuring and Monitoring OC-3 and OC-12 (SONET) Ports

Both OC-3 and OC-12 (SONET) network modules are supported. To configure, check the status of, and view statistics for OC-3 and OC-12 ports, select the OC-3 or OC-12 port(s) from a front panel, pull down the **`Configure/Port`** menu, and launch the OCx Control / Monitor dialog. The OCx Control / Monitor dialog is shown in the following figure:



ForeView - Port D1 OCx Control / Monitor - crabcake

Port Control

Framing: SONET
Loopback: NoLoop
Clock Source: localTiming
Scrambling: on
Empty Cell: unassigned

OCx Status

Section Status: 1
○ LOS
○ LOF

Line Status: 1
○ AIS
○ FERF

Path Status: 1
○ LOP
○ AIS
○ Yellow

OCx Statistics

Section
BIP-8s: 160102136
LOSs: 2086
LOFs: 2086

Line
BIP-24s: 1249
FEBEs: 12898
AISs: 2086
FERFs: 1

Path
BIP-8s: 554
FEBEs: 4966
LOPs: 0
AISs: 2086
Yellows: 2087

Header Check
Correctable: 0
Uncorrectable: 121

Figure 8.10 - OCx Control / Monitor Dialog

The OCx Control / Monitor dialog has three divisions. They are Port Control, OCx Status, and OCx Statistics. The following sections define the various menu items of each division.

8.10.1 Port Control

The fields in this section of the display are defined as follows:

Framing Allows selection between Synchronous Optical Network (SONET) and Synchronous Digital Hierarchy (SDH) framing.

Loopback Indicates the loopback mode on this port, which can be one of the following: **`NoLoop`**, **`LineLoop`**, or **`DiagLoop`**. **`NoLoop`** means that no loopback will occur on this port. **`LineLoop`** causes the received data and clock to be directly transmitted back out; this is useful to help the remote side perform diagnostics. **`DiagLoop`** connects the transmitter of the local port to its own receiver; this can be used to test the function of the local hardware.

Clock Source Allows the transmission hardware clock to be based on the internal OCx clock (**`local Timing`**) or based on the timing signal regenerated from the received input stream (**`rx Timing`**).

Scrambling **`On`** indicates that payload scrambling is enabled on this port. **`Off`** means that payload scrambling is disabled on this port.

Empty Cell Indicates the type of cells this port will send for filler when the port is not sending data. Idle means the CLP bit = 1. Unassigned means the CLP bit = 0. Please refer to page 57 of the ATM Forum 3.0 Specification for more information.

8.10.2 OCx Status

The fields in this section of the display are defined as follows:

Section Status Indicates the OCx section status of the port.

LOS Indicates if a Loss Of Signal (LOS) is occurring. A LOS is declared when 20 +/- 3us of all zeros patterns is detected. LOS is cleared when two valid framing words are detected and during the intervening time no LOS condition is detected.

LOF Indicates if a Loss Of Frame (LOF) is occurring. A LOF is declared when an out-of-frame (OOF) condition persists for 3ms. The LOF is cleared when an in-frame condition persists for 3ms. While in-frame the framing bytes (A1, A2) in each frame are compared against the expected pattern. Out-of-frame is declared when four consecutive frames containing one or more framing pattern errors have been received.

Line Status Indicates the OCx line status of the port.

AIS Indicates if an Alarm Indication Signal (AIS) is occurring. A line AIS is asserted when a 111 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line AIS is removed when any pattern other than 111 is detected in these bits for five consecutive frames.

FERF Indicates if a line Far End Receive Failure (FERF) is occurring. A line FERF is asserted when a 110 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line FERF is removed when any pattern other than 110 is detected in these bits for five consecutive frames.

Path Status Indicates the OCx path status of the port.

LOP Indicates if a path Loss Of Pointer (LOP) is occurring. A path LOP is detected when a “normal pointer value” is not found in eight consecutive frames. The LOP is cleared when a “normal pointer value” is detected for three consecutive frames.

AIS Indicates if a path Alarm Indication Signal (AIS) is occurring. A path AIS is asserted when an all-ones pattern is detected in the pointer bytes (H1 and H2) for three consecutive frames. It is cleared when a valid pointer is detected for three consecutive frames. AIS indicates that an upstream failure has been detected.

Yellow Shows the number of seconds in which path yellow alarm is occurring. A path yellow alarm is detected by extracting bit 5 of the path status byte. If bit 5 is high for ten consecutive frames, a yellow alarm is declared. A yellow alarm is cleared when bit 5 is low for ten consecutive frames. Yellow signals are used to alert upstream terminals of a downstream failure in order to initiate trunk conditioning on the failure circuit.

8.10.3 OCx Statistics

The fields in this section of the display are defined as follows:

8.10.3.1 Section

BIP-8s Shows the number of Section BIP-8 (Bit Interleaved Parity) errors that have been detected since the last time the port has been reset. The calculated BIP-8 code is compared with the BIP-8 code extracted from the B1 byte of the following frame. Differences indicate that a section level bit error is occurring.

LOSs Displays the number of seconds in which Loss Of Signal (LOS) is occurring. A LOS is declared when 20 +/- 3us of all zeros patterns is detected. LOS is cleared when two valid framing words are detected and during the intervening time no LOS condition is detected.

LOFs Specifies the number of seconds in which Loss Of Frame (LOF) is occurring. A LOF is declared when an out-of-frame (OOF) condition persists for 3ms. The LOF is cleared when an in-frame condition persists for 3ms. While in-frame the framing bytes (A1, A2) in each frame are compared against the expected pattern. Out-of-frame is declared when four consecutive frames containing one or more framing pattern errors have been received.

Line

BIP-24s Indicates the number of Line BIP-24 (Bit Interleaved Parity) errors that have been detected since the last time the port has been reset. The calculated BIP-24 code is based on the line overhead and synchronous payload envelope (SPE) of the STS-3c stream. The line BIP-24 code is a bit interleaved parity calculation using even parity. The calculated code is compared with the BIP-24 code extracted from the B2 bytes of the following frame. Differences indicate that a line layer bit error has occurred.

FEBEs Lists the number of line Far End Block Errors (FEBE) that have been detected since the last time the port has been reset.

AISs Shows the number of seconds in which line Alarm Indication Signal (AIS) has occurred. A line AIS is asserted when a 111 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line AIS is removed when any pattern other than 111 is detected in these bits for five consecutive frames.

FERFs Specifies the number of seconds in which line Far End Receive Failure (FERF) has occurred. A line FERF is asserted when a 110 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line FERF is removed when any pattern other than 110 is detected in these bits for five consecutive frames.

8.10.3.2 Path

BIP-8s Indicates the number of Path BIP-8 (Bit Interleaved Parity) errors that have been detected since the last time the port has been reset. A path BIP-8 error is detected by comparing the path BIP-8 byte (B3) extracted from the current frame, to the path BIP-8 computed for the previous frame.

FEBEs Displays the number of path Far End Block Errors (FEBE) that have been detected since the last time the port has been reset. FEBEs are detected by extracting the 4-bit FEBE field from the path status byte (G1). The legal range for the 4-bit field is between 0000 and 1000, representing zero to eight errors. Any other value is interpreted as zero errors.

LOPs Lists the number of seconds in which path Loss Of Pointer (LOP) has occurred. A path LOP is detected when a “normal pointer value” is not found in eight consecutive frames. The LOP is cleared when a “normal pointer value” is detected for three consecutive frames.

AISs Indicates the number of seconds in which path Alarm Indication Signal (AIS) has occurred. A path AIS is asserted when an all-ones pattern is detected in the pointer bytes (H1 and H2) for three consecutive frames. It is cleared when a valid pointer is detected for three consecutive frames. AIS indicates that an upstream failure has been detected.

Yellows Shows the number of seconds in which path yellow alarm has occurred. A path yellow alarm is detected by extracting bit 5 of the path status byte. If bit 5 is high for ten consecutive frames, a yellow alarm is declared. A yellow alarm is cleared when bit 5 is low for ten consecutive frames. Yellow signals are used to alert upstream terminals of a downstream failure in order to initiate trunk conditioning on the failure circuit.

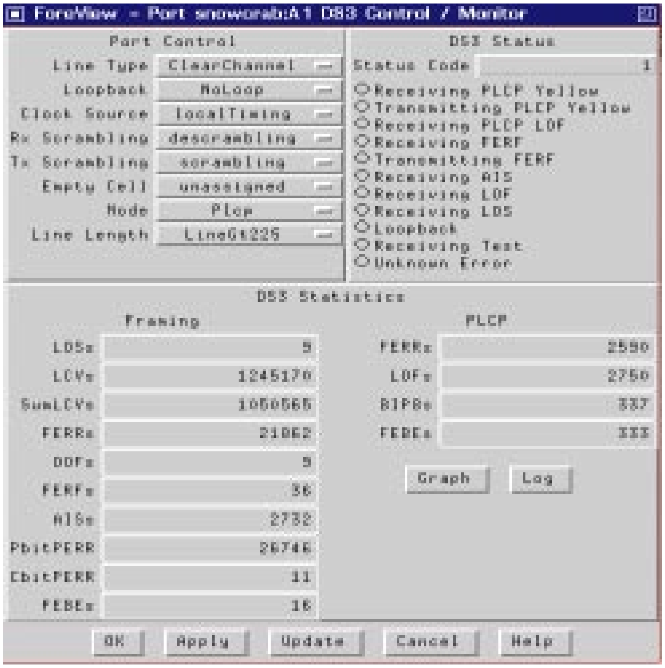
8.10.3.3 Header Check

Correctable Lists the number of correctable Header Check Sequence (HCS) error events that occurred since the port was reset. The HCS is a CRC-8 calculation over the first 4 octets of the ATM cell header.

Uncorrectable Displays the number of uncorrectable Header Check Sequence (HCS) error events that occurred since the port was reset. The HCS is a CRC-8 calculation over the first 4 octets of the ATM cell header.

8.11 Configuring and Monitoring DS-3 Ports

To configure, check the status of, and view statistics for DS-3 ports, select the DS-3 port(s) from a front panel, pull down the **`Configure/Port`** menu, and launch the **`DS-3 Control/Monitor`** dialog. The **`DS-3 Control/Monitor`** dialog is shown in the following figure:



ForeView - Port snowcrab:A1 DS3 Control / Monitor

Port Control

Line Type	ClearChannel
Loopback	NoLoop
Clock Source	localTiming
Rx Scrambling	descrambling
Tx Scrambling	scrambling
Empty Cell	unassigned
Mode	Plcp
Line Length	LineGt225

DS3 Status

Status Code 1

- ○ Receiving PLCP Yellow
- ○ Transmitting PLCP Yellow
- ○ Receiving PLCP LOF
- ○ Receiving FERF
- ○ Transmitting FERF
- ○ Receiving AIS
- ○ Receiving LOF
- ○ Receiving LOS
- ○ Loopback
- ○ Receiving Test
- ○ Unknown Error

DS3 Statistics

Framing

LOSs	5
LCVs	1245170
SumLCVs	1050565
FERRs	21062
OOFs	5
FERFs	36
AISs	2732
PbitPERR	26746
CbitPERR	11
FEBEs	16

PLCP

FERRs	2590
LOFs	2750
BIP8s	337
FEBEs	333

Figure 8.11 - DS-3 Control / Monitor Dialog

The **`DS-3 Control/Monitor`** dialog has three divisions. They are Port Control, DS-3 Status, and DS-3 Statistics. The following sections define the various menu items of each division.

8.11.1 Port Control

The fields in this section of the display are defined as follows:

Line Type Allows a choice between two types of transmission for the DS-3 signal. **`CbitParity`** is recommended by the ATM Forum for DS-3 communications, but **`ClearChannel`** is sometimes needed when connecting to third party equipment.

Loopback Indicates the loopback mode on this port and can be one of the following: **`NoLoop`**, **`CellLoop`**, **`PayloadLoop`**, **`DiagLoop`**, or **`LineLoop`**. **`CellLoop`** causes the received data to be immediately retransmitted on a cell-by-cell basis. **`PayloadLoop`** causes the received data to be immediately retransmitted on a DS-3 payload by payload basis. **`DiagLoop`** causes the received data stream and clock to be immediately retransmitted without regard to reframing or cell delineation. **`LineLoop`** causes the received data and clock to be directly transmitted back out; this is useful to help the remote side perform diagnostics.

Clock Source Allows the transmission hardware clock to be based on the internal DS-3 clock (**`local Timing`**) or based on the timing signal regenerated from the received input stream (**`rx Timing`**).

Rx Scrambling Enables or disables the descrambling of the payload in all received frames. This should be set to match the transmit scrambling chosen by the remote connection.

Tx Scrambling Enables or disables the payload scrambling for all transmitted frames. Payload scrambling can be used when there is not a sufficient “ones density” on the transmission line, which can sometimes cause trouble on wide-area links.

Mode Type of framing enabled on this port. Options are Plcp or Hcs.

Empty Cell Indicates the type of cells this port will send for filler when the port is not sending data. Idle means the CLP bit = 1. Unassigned means the CLP bit = 0. Please refer to page 57 of the ATM Forum 3.0 Specification for more information.

Line Length This variable represents the length of the physical cable connected to the DS-3 port. The user has to set this object to match the physical cable length so that the network module can receive the signal on the cable. **`LineLt225`** means the line is shorter than 255 ft. **`LineGt225`** means the line is longer than 220 ft. This option is valid for Series C network modules only.

8.11.2 DS-3 Status

The fields in this section of the display are defined as follows:

Status Code Bit-mapped representation of error conditions on the port. A value of 1 means no errors reported.

Receiving PLCP Yellow Yellow alarm errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver. The yellow alarm is asserted when 10 consecutive yellow signal bits are set to logical 1.

Transmitting PLCP Yellow Yellow signals are generated by the PLCP (Physical Layer Convergence Protocol) transmitter to alert upstream terminals of a downstream failure in order to initiate trunk conditioning on the failure circuit.

Receiving PLCP LOF Loss Of Frame (LOF) errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver.

Receiving FERF Far End Receive Failure (FERF) state has been detected by the DS-3 Receive Framer block.

Transmitting FERF Far End Receive Failure (FERF) state has been detected by the DS-3 Receive Framer block.

Receiving AIS Alarm Indication Signals (AIS) were detected by the DS-3 Receive Framer block.

Receiving LOF Loss Of Frame (LOF) errors were detected by the DS-3 Receive Framer block.

Receiving LOS Loss Of Signal (LOS) errors were detected by the DS-3 Receive Framer block.

Loopback Loopback errors were detected on this port.

Receiving Test Receiving test failure has been detected.

Unknown Error An error of unknown origin has occurred.

8.11.3 DS-3 Statistics

The fields in this section of the display are defined as follows:

8.11.3.1 Framing

LOSs Specifies the number of seconds in which Loss Of Signal (LOS) errors were detected by the DS-3 Receive Framer block.

LCVs Indicates the number of Line Code Violations (LCV) that were detected by the DS-3 Receive Framer block.

SumLCVs Shows the number of DS-3 information blocks (85 bits) which contain one or more Line Code Violations (LCV).

FERRs Displays the number of DS-3 framing error (FERR) events.

OOFs Specifies the number of DS-3 Out Of Frame (OOF) error events.

FERFs Indicates the number of seconds in which a Far End Receive Failure (FERF) state has been detected by the DS-3 Receive Framer block. The FERF signal alerts the upstream terminal that a failure has been detected along the downstream line.

AISs Shows the number of seconds in which Alarm Indication Signals (AIS) were detected by the DS-3 Receive Framer block. AIS indicates that an upstream failure has been detected by the far end.

PbitPERRs Displays the number of P-bit parity error (PERR) events.

CbitPERRs Specifies the number of C-bit parity error (PERR) events.

FEBEs Indicates the number of DS-3 far end block error (FEBE) events.

8.11.3.2 PLCP

FERRs Lists the number of Physical Layer Convergence Protocol (PLCP) octet error events.

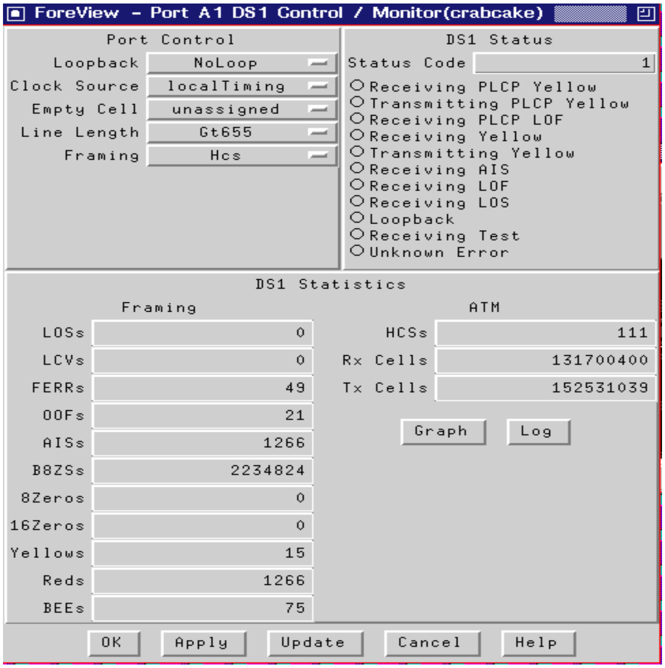
LOFs Shows the number of seconds in which Loss Of Frame (LOF) errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver. LOF is declared when an Out-Of-Frame state persists for more than 1ms. LOF is removed when an in-frame state persists for more than 12ms.

BIP8s Displays the number of BIP-8 (Bit Interleaved Parity-8) error events. The BIP-8 is calculated over the Path Overhead field and the associated ATM cell of the previous frame. A BIP-N is a method of error monitoring. An N-bit code is generated by the transmitting equipment in such a manner that the first bit of the code provides even parity over the first bit of all N-bit sequences in the previous VT SPE, the second bit provides even parity over the second bits of all N-bit sequences within the specified portion, etc.

FEBEs Specifies the number of ATM Far End Block Error (FEBE) events.

8.12 Configuring and Monitoring DS-1 Ports

To configure, check the status of, and view statistics for DS-1 ports, select the DS-1 port(s) from a front panel, pull down the **`Configure/Port`** menu, and launch the **`DS-1 Control/Monitor`** dialog. The **`DS-1 Control/Monitor`** dialog is shown in the following figure:



ForeView - Port A1 DS1 Control / Monitor(crabcake)

Port Control

Loopback	NoLoop
Clock Source	localTiming
Empty Cell	unassigned
Line Length	Gt655
Framing	Hcs

DS1 Status

Status Code: 1

○ Receiving PLCP Yellow
○ Transmitting PLCP Yellow
○ Receiving PLCP LOF
○ Receiving Yellow
○ Transmitting Yellow
○ Receiving AIS
○ Receiving LOF
○ Receiving LOS
○ Loopback
○ Receiving Test
○ Unknown Error

DS1 Statistics

Framing		ATM	
LOSs	0	HCSs	111
LCVs	0	Rx Cells	131700400
FERRs	49	Tx Cells	152531039
OOFs	21		
AISs	1266		
B8ZSs	2234824		
8Zeros	0		
16Zeros	0		
Yellows	15		
Reds	1266		
BEEs	75		

Figure 8.12 - DS-1 Control/Monitor Dialog

The **`DS-1 Control/Monitor`** dialog has three divisions. They are Port Control, DS-1 Status, and DS-1 Statistics. The following sections define the various menu items of each division.

8.12.1 Port Control

The fields in this section of the display are defined as follows:

Loopback Indicates the loopback mode on this port. Can be one of the following: **NoLoop**, **LineLoop**, **PayloadLoop**, or **DiagLoop**. **NoLoop** means that no loopback will occur on this port. **LineLoop** causes the received data and clock to be directly transmitted back out; this is useful to help the remote side perform diagnostics. **PayloadLoop** causes the received data to be immediately retransmitted on a DS-1 payload by payload basis. **DiagLoop** causes the received data stream and clock to be immediately retransmitted without regard to reframing or cell delineation.

Clock Source Allows the transmission hardware clock to be based on the internal DS-1 clock (**local Timing**) or based on the timing signal regenerated from the received input stream (**rx Timing**)

Empty Cell Indicates the type of cells this port sends for filler when the port is not sending data. Idle means the CLP bit = 1. Unassigned means the CLP bit = 0. Please refer to page 57 of the ATM Forum 3.0 Specification for more information.

Line Length This variable represents the length of the physical cable connected to the DS-1 port, measured in feet. The user has to set this object to match the physical cable length so that the network module can receive the signal on the cable. **Lt110** means the line is shorter than 110 ft. **Lt655** means the line is greater than 655 feet.

Mode Indicates the type of framing used for the port. Can be **Hcs** or **Plcp**. The default mode of operation is **Hcs**.

8.12.2 DS-1 Status

The fields in this section of the display are defined as follows:

Status Code Bit-mapped representation of error conditions on the port. A value of 1 means no errors reported.

Receiving PLCP Yellow Yellow alarm errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver. The yellow alarm is asserted when 10 consecutive yellow signal bits are set to logical 1.

Transmitting PLCP Yellow Yellow signals are generated by the PLCP (Physical Layer Convergence Protocol) transmitter to alert upstream terminals of a downstream failure in order to initiate trunk conditioning on the failure circuit.

Receiving PLCP LOF Loss Of Frame (LOF) errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver.

Receiving Yellow Yellow alarm errors were detected by the DS-1 Receive Framer block.

Transmitting Yellow Yellow signals are used to alert upstream terminals of a downstream failure in order to initiate trunk conditioning on the failure circuit.

Receiving AIS Alarm Indication Signals (AIS) were detected by the DS-1 Receive Framer block.

Receiving LOF Loss Of Frame (LOF) errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver.

Receiving LOS Loss Of Signal (LOS) errors were detected by the DS-1 Receive Framer block.

Loopback Loopback errors were detected on this port.

Receiving Test Receiving test failure has been detected.

Unknown Error An error of unknown origin has occurred.

8.12.3 DS-1 Statistics

The fields in this section of the display are defined as follows:

8.12.3.1 Framing

LOSs Specifies the number of seconds in which Loss Of Signal (LOS) errors were detected by the DS-1 Receive Framer block.

LCVs Indicates the number of Line Code Violations (LCV) that were detected by the DS-1 Receive Framer block.

FERRs Displays the number of DS-1 framing error (FERR) events.

OOFs Specifies the number of DS-1 Out Of Frame (OOF) error events.

AISs Shows the number of seconds in which Alarm Indication Signals (AIS) were detected by the DS-1 Receive Framer block. AIS indicates that an upstream failure has been detected by the far end.

B8ZSs Displays the number of B8ZS pattern error events.

8Zeros Lists the number of 8-zero error events.

16Zeros Shows the number of 16-zero error events.

Yellows Indicates the number of Yellow Alarm events.

Reds Displays the number of Red Alarm events.

BEEs Lists the number of Bit Encoding Error (BEE) events.

8.12.3.2 ATM

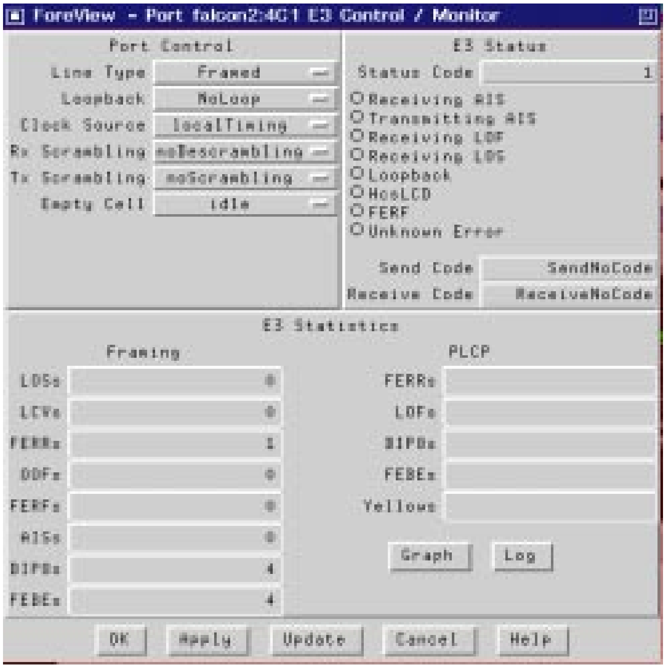
HCSs Shows the number of header check sequence (HCS) error events. The HCS is a CRC-8 calculation over the first 4 octets of the ATM cell header.

Rx Cells Indicates the number of ATM cells received.

Tx Cells Lists the number of transmitted non-null ATM cells.

8.13 Configuring and Monitoring E-3 Ports

To configure, check the status of, and view statistics for E-3 ports, select the E-3 port(s) from a front panel, pull down the **`Configure/Port`** menu, and launch the **`E-3 Control/Monitor`** dialog. The **`E-3 Control/Monitor`** dialog is shown in the following figure:



ForeView - Port falcon2:4C1 E3 Control / Monitor

Port Control

Line Type: Framed
Loopback: NoLoop
Clock Source: localTiming
Rx Scrambling: noDescrambling
Tx Scrambling: noScrambling
Empty Cell: idle

E3 Status

Status Code: 1

○ Receiving AIS
○ Transmitting AIS
○ Receiving LOF
○ Receiving LOS
○ Loopback
○ HcsLCD
○ FERF
○ Unknown Error

Send Code: SendNoCode
Receive Code: ReceiveNoCode

E3 Statistics

Framing		PLCP	
LOSs	0	FERRs	
LCVs	0	LOFs	
FERRs	1	BIPDs	
OOFs	0	FEBEs	
FERFs	0	Yellows	
AISs	0		
BIPBs	4		
FEBEs	4		

Figure 8.13 - E-3 Control / Monitor Dialog

The **`E-3 Control/Monitor`** dialog has three divisions. They are Port Control, E-3 Status, and E-3 Statistics. The following sections define the various menu items of each division.

8.13.1 Port Control

The fields in this section of the display are defined as follows:

Line Type This variable indicates the type of cell delineation being used. The Plcp value indicates cell delineation according to CCITT G.751 using PLCP (Physical Layer Convergence Protocol) framing, while Framed indicates HCS (Header Check Sequence) based framing.

Loopback Indicates the loopback mode on this port and can be one of the following: **`NoLoop`**, **`CellLoop`**, **`PayloadLoop`**, **`DiagLoop`**, or **`LineLoop`**. **`CellLoop`** causes the received data to be immediately retransmitted on a cell-by-cell basis. **`PayloadLoop`** causes the received data to be immediately retransmitted on a E-3 payload by payload basis. **`DiagLoop`** causes the received data stream and clock to be immediately retransmitted without regard to reframing or cell delineation. **`LineLoop`** causes the received data and clock to be directly transmitted back out; this is useful to help the remote side perform diagnostics.

Clock Source Allows the transmission hardware clock to be based on the internal E-3 clock (**`local Timing`**) or based on the timing signal regenerated from the received input stream (**`rx Timing`**)

Rx Scrambling This variable indicates whether the information is being descrambled when it is received. It should be set the same as the transmitting side.

Tx Scrambling This variable indicates whether the information (48-octet payload) is being scrambled before transmitting. It should be set the same as the receiving side.

Empty Cell Indicates the type of cells this port sends for filler when the port is not sending data. Idle means the CLP bit = 1. Unassigned means the CLP bit = 0. Please refer to page 57 of the ATM Forum 3.0 Specification for more information.

8.13.2 E-3 Status

The fields in this section of the display are defined as follows:

Status Code Bit-mapped representation of error conditions on the port. A value of 1 means no errors reported.

Receiving AIS Alarm Indication Signals (AIS) were detected by the DS-1 Receive Framer block.

Transmitting AIS AIS are transmitted upstream to alert that a failure has been detected by the far end.

Receiving LOF Loss Of Frame (LOF) errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver.

Receiving LOS Loss Of Signal (LOS) errors were detected by the DS-1 Receive Framer block.

Loopback Loopback errors were detected on this port.

HcsLCD Loss of Cell Delineation.

FERF Receiving Far End Receive Failure.

Unknown Error An error of unknown origin has occurred.

Send Code This variable indicates what type of code is being sent across the E-3 interface by the device. The values are: NoCode, which means sending looped or normal data; LineCode, which means sending request for a line loopback; and PayloadCode, which means sending a request for a payload loopback (i.e. all DS-1/E-1 in a E-3/E-3 frame).

Receive Code This variable indicates the type of code that was received across the E-3 interface. The values mean: NoCode (1), receiving looped or normal data; LineCode (2), receiving request for a line loopback; PayloadCode (3), receiving a request for a payload loopback; ResetCode (4), receiving a loopback deactivation request; LoopCode (5), receiving a request to loopback within a E-3/E-3 frame; TestPattern (6), receiving a test pattern.

8.13.3 E-3 Statistics

The fields in this section of the display are defined as follows:

8.13.3.1 Framing

LOSs Specifies the number of seconds in which Loss Of Signal (LOS) errors were detected by the E-3 Receive Framer block.

LCVs Indicates the number of Line Code Violations (LCV) that were detected by the DS-3 Receive Framer block.

FERRs Displays the number of E-3 framing error (FERR) events.

OOFs Specifies the number of E-3 Out Of Frame (OOF) error events.

FERFs Indicates the number of Far End Receive Failures for a port configured with HCS framing. Indicates the number of Remote Alarm Indications for a port configured with PLCP framing.

AISs Shows the number of seconds in which Alarm Indication Signals (AIS) were detected by the E-3 Receive Framer block. AIS indicates that an upstream failure has been detected by the far end.

BIP8s Shows the number of E-3 G.832 BIP-8 errors. This counter is only valid for a port configured with HCS framing.

FEBEs Displays the number of E-3 far end block error (FEBE) events.

8.13.3.2 PLCP

FERRs Lists the number of Physical Layer Convergence Protocol (PLCP) octet error events.

LOFs Indicates the number of seconds in which Loss Of Frame (LOF) errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver. LOF is declared when an Out-Of-Frame state persists for more than 1ms. LOF is removed when an in-frame state persists for more than 12ms.

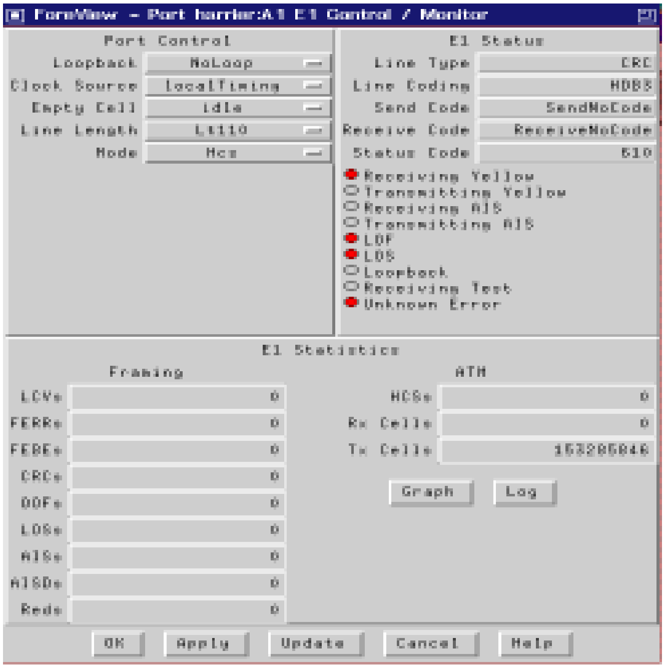
BIP8s Specifies the number of BIP-8 (Bit Interleaved Parity-8) error events. The BIP-8 is calculated over the Path Overhead field and the associated ATM cell of the previous frame. A BIP-N is a method of error monitoring. An N-bit code is generated by the transmitting equipment in such a manner that the first bit of the code provides even parity over the first bit of all N-bit sequences in the previous VT SPE, the second bit provides even parity over the second bits of all N-bit sequences within the specified portion, etc.

FEBEs Displays the number of ATM Far End Block Error (FEBE) events.

Yellows Shows the number of seconds in which Yellow alarm errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver. Yellow alarm is asserted when 10 consecutive yellow signal bits are set to logical 1. Yellow signals are used to alert upstream terminals of a downstream failure in order to initiate trunk conditioning on the failure circuit.

8.14 Configuring and Monitoring E-1 Ports

To configure, check the status of, and view statistics for E-1 ports, select the E-1 port(s) from a front panel, pull down the **`Configure/Port`** menu and launch the E-1 Control / Monitor dialog. The E-1 Control / Monitor dialog is shown in the following figure:


ForeView - Port harrier:A1 E1 Control / Monitor

Port Control

Loopback: NoLoop
Clock Source: LocalTiming
Empty Cell: Idle
Line Length: Lt110
Mode: Hcs

E1 Status

Line Type: CRC
Line Coding: HDB3
Send Code: SendNoCode
Receive Code: ReceiveNoCode
Status Code: 610

● Receiving Yellow
○ Transmitting Yellow
○ Receiving AIS
○ Transmitting AIS
● LOF
● LOS
○ Loopback
○ Receiving Test
● Unknown Error

E1 Statistics

Framing

LCVs: 0
FERRs: 0
FEBEs: 0
CRCs: 0
OOFs: 0
LOSs: 0
AISs: 0
AISDs: 0
Reds: 0

ATM

HCSs: 0
Rx Cells: 0
Tx Cells: 153205846

Figure 8.14 - E-1 Control / Monitor Dialog

The E-1 Control / Monitor dialog has three divisions. They are Port Control, E-1 Status, and E-1 Statistics. The following sections define the various menu items of each division.

8.14.1 Port Control

The fields in this section of the display are defined as follows:

Loopback Indicates the loopback mode on this port. Can be one of the following: NoLoop, cell, payload, or diagnostic. Cell loopback causes the received data to be immediately retransmitted on a cell-by-cell basis. Payload loopback causes the received data to be immediately retransmitted on a E-1 payload by payload basis. Diagnostic loopback causes the received data stream and clock to be immediately retransmitted without regard to reframing or cell delineation.

Clock Source Allows the transmission hardware clock to be based on the internal E-1 clock (internal) or based on the timing signal regenerated from the received input stream (received).

Empty Cell Indicates the type of cells this port will send for filler when the port is not sending data. Idle means the CLP bit = 1. Unassigned means the CLP bit = 0. Please refer to page 57 of the ATM Forum 3.0 Specification for more information.

Line Length This variable represents the length of the physical cable connected to the E-1 port. The user has to set this object to match the physical cable length so that the network module can receive the signal on the cable. The possible values are: LineLt110 (1) means the line is shorter than 110 ft.; Line110-220 (2) means the line is between 110 and 220 ft.; Line220-330 (3) means the line is between 220 and 330 ft.; Line330-440 (4) means the line is between 330 and 440 ft.; Line440-550 (5) means the line is between 440 and 550 ft.; Line550-660 (6) means the line is between 550 and 660 ft.; LineG703-75 (7) G703 standard (75 ohm coaxial line); LineG703-120 (8) G703 standard (120 ohm symmetrical line).

8.14.2 Port Status

The fields in this section of the display are defined as follows:

Line Type This variable indicates the variety of E-1 Line implementing this circuit. The type of circuit affects the number of bits per second that the circuit can reasonably carry, as well as the interpretation of the usage and error statistics. This variable is defined in the RFC1406 configuration table as dsx1LineType. According to RFC1406, the different values are: NoCRC CCITT recommendation G.704 (Table A); CRC CCITT recommendation G.704 (Table B); MF G.704 (Table A) with TS16 multiframing enabled MFCRC G.704 (Table B) with TS16 multiframing enabled.

Line Coding This variable indicates the type of code that was used on the E-1 interface. The values mean: NoCode, receiving looped or normal data; LineCode, receiving request for a line loopback; PayloadCode, receiving a request for a payload loopback; ResetCode, receiving a loopback deactivation request; QRS, receiving a Quasi-Random Signal (QRS); test pattern, 511Patternreceiving a 511 bit fixed test pattern; 3in24Pattern, receiving a fixed test pattern of 3 bits set in 24; OtherTestPattern, receiving a test pattern other than the above.

Send Code This variable indicates the type of code that was sent across the E-1 interface. (See Line Coding).

Receive Code This variable indicates the type of code that was received across the E-1 interface. (See Line Coding).

Status Code Bit-mapped representation of error conditions on the port. A value of 1 means no errors reported.

Receiving Yellow Yellow alarm errors were detected by the E-1 Receive Framer block.

Transmitting Yellow Yellow signals are used to alert upstream terminals of a downstream failure in order to initiate trunk conditioning on the failure circuit.

Receiving AIS Alarm Indication Signals (AIS) were detected by the DS-1 Receive Framer block.

Transmitting AIS AIS are transmitted upstream to alert that a failure has been detected by the far end.

LOF Loss of Frame (LOF) errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver.

LOS Loss Of Signal (LOS) errors were detected by the DS-1 Receive Framer block.

Loopback Loopback errors were detected on this port.

Receiving Test This variable indicates the type of code that was received across the E-3 interface. The values mean: NoCode (1), receiving looped or normal data; LineCode(2), receiving request for a line loopback; PayloadCode (3), receiving a request for a payload loopback; ResetCode (4), receiving a loopback deactivation request; LoopCode (5), receiving a request to loopback within a E-3/E-3 frame; TestPattern (6), receiving a test pattern.

Unknown Error An error of unknown origin has occurred.

8.14.3 E-1 Statistics

The fields in this section of the display are defined as follows:

8.14.3.1 Framing

LCVs Indicates the number of Line Code Violations (LCV) that were detected by the E-1 Receive Framer block.

FERRs Displays the number of E-1 framing error (FERR) events.

FEBEs Indicates the number of E-1 far end block errors.

CRCs Displays the number of cyclic redundancy errors.

OOFs Specifies the number of E-1 Out Of Frame (OOF) error events.

LOSs Specifies the number of seconds in which Loss Of Signal (LOS) errors were detected by the E-1 Receive Framer block.

AISs Shows the number of seconds in which Alarm Indication Signals (AIS) were detected by the E-1 Receive Framer block. AIS indicates an upstream failure has been detected by the far end.

AISDs Displays the number of AISD (unframed pattern of all ones) error events.

Reds Shows the number of Red Alarm events.

8.14.3.2 ATM

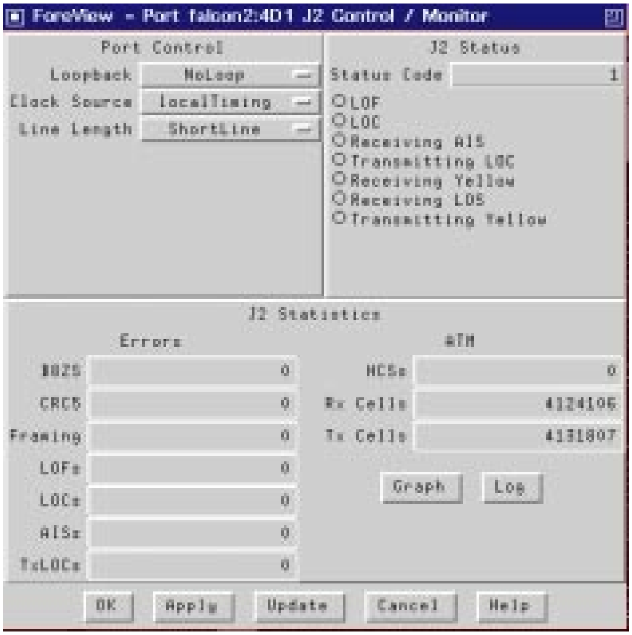
HCSs Lists the number of header check sequence (HCS) error events. The HCS is a CRC-8 calculation over the first 4 octets of the ATM cell header.

Rx Cells Shows the number of ATM cells that were received.

Tx Cells Indicates the number of non-null ATM cells that were transmitted.

8.15 Configuring and Monitoring J-2 Ports

To configure, check the status of, and view statistics for J-2 ports, select the J-2 port(s) from a front panel, pull down the **`Configure/Port`** menu and launch the J-2 Control / Monitor dialog. The J-2 Control / Monitor dialog is shown in the following figure:



Loopback: NoLoop
Clock Source: localTiming
Line Length: ShortLine

Status Code: 1

○ LOF
○ LOC
○ Receiving AIS
○ Transmitting LOC
○ Receiving Yellow
○ Receiving LOS
○ Transmitting Yellow

Errors		ATM	
B8ZS	0	HCSs	0
CRC5	0	Rx Cells	4124106
Framing	0	Tx Cells	4131807
LOFs	0		
LOCs	0		
AISs	0		
TxLOCs	0		

Figure 8.15 - J-2 Control / Monitor Dialog

The J-2 Control / Monitor dialog has three divisions. They are Port Control, J-2 Status, and J-2 Statistics. The following sections define the various menu items of each division.

8.15.1 Port Control

The fields in this section of the display are defined as follows:

Loopback Indicates the loopback mode on this port and can be one of the following: **`NoLoop,`** **`DiagLoop,`** or **`LineLoop`**. **`DiagLoop`** causes the received data stream and clock to be immediately retransmitted without regard to reframing or cell delineation. **`LineLoop`** causes the received data and clock to be directly transmitted back out; this is useful to help the remote side perform diagnostics.

Clock Source Allows the transmission hardware clock to be based on the internal J-2 clock (**`local Timing`**) or based on the timing signal regenerated from the received input stream (**`rx Timing`**).

Line Length Indicates the length of the physical cable attached to this port. If the line attached to the receive port has greater than 4 db of attenuation, then the line must be configured as long. If otherwise, then it must be configured as short. In general, if the cable is less than 20 feet, then configure the line as short.

8.15.2 J-2 Status

The fields in this section of the display are defined as follows:

Status Code Bit-mapped representation of error conditions on the port. A value of 1 means no errors have been reported.

LOF Loss of Frame.

LOC Loss of Clock.

Receiving AIS Receive Alarm Indication Signal.

Transmitting LOC Transmit Loss of Clock.

Receiving Yellow Yellow alarm errors were detected by the J-2 Receive Framer block.

Receiving LOS Loss Of Signal (LOS) errors were detected by the J-2 Receive Framer block.

Transmitting Yellow Yellow signals are used to alert upstream terminals of a downstream failure in order to initiate trunk conditioning on the failure circuit.

8.15.3 J-2 Statistics

The fields in this section of the display are defined as follows:

8.15.3.1 Errors

B8ZS Displays the number of B8ZS coding violation errors.

CRC5 Shows the number of CRC-5 received errors.

Framing Lists the number of framing patterns received in error.

LOFs Shows the number of seconds in which Loss Of Frame (LOF) errors were detected by the PLCP (Physical Layer Convergence Protocol) receiver. LOF is declared when an Out-Of-Frame state persists for more than 1ms. LOF is removed when an in-frame state persists for more than 12ms.

LOCs Shows the number of seconds in which Loss Of Clock (LOC) errors were detected by the PLCP.

AISs Shows the number of seconds in which Alarm Indication Signals (AIS) were detected by the J-2 Framer block.

TxLOCs Shows the number of seconds during which the transmitter was experiencing Loss Of Clock.

8.15.3.2 ATM

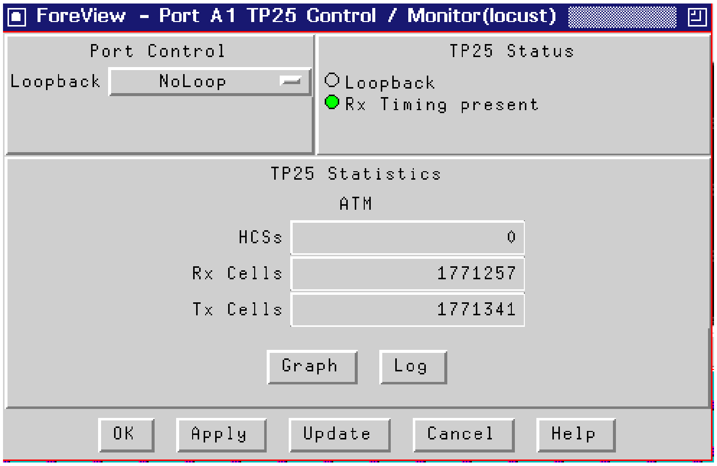
HCSs Indicates the number of header check sequence (HCS) error events. The HCS is a CRC-8 calculation over the first 4 octets of the ATM cell header.

RxCells Displays the number of ATM cells that were received.

TxCells Show the number of non-null ATM cells that were transmitted.

8.16 Configuring and Monitoring TP-25 Ports

To configure, check the status of, and view statistics for TP-25 ports, select the TP-25 port(s) from a front panel, pull down the **`Configure/Port`** menu and launch the TP-25 Control/ Monitor dialog. The TP-25 Control/Monitor dialog is shown in the following figure:



Loopback: NoLoop

○ Loopback
● Rx Timing present

HCSs	0
Rx Cells	1771257
Tx Cells	1771341

Figure 8.16 - TP-25 Control/Monitor Dialog

The TP-25 Control/Monitor dialog has three divisions. They are Port Control, TP-25 Status, and TP-25 Statistics. The following sections define the various menu items of each division.

8.16.1 Port Control

The fields in this section of the display are defined as follows:

Loopback Indicates the loopback mode on this port and can be one of the following: **`NoLoop`**, **`DiagLoop`**, or **`LineLoop`**. **`DiagLoop`** causes the received data stream and clock to be immediately retransmitted without regard to reframing or cell delineation. **`LineLoop`** causes the received data and clock to be directly transmitted back out; this is useful to help the remote side perform diagnostics.

8.16.2 TP-25 Status

The fields in this section of the display are defined as follows:

Loopback Indicates that the TP25 port is in line loopback mode. When a TP25 port is in loopback mode, it no longer passes normal traffic

Rx Timing present Indicates that the timing signal is regenerated from the received input stream.

8.16.3 TP-25 Statistics

The fields in this section of the display are defined as follows:

8.16.3.1 ATM

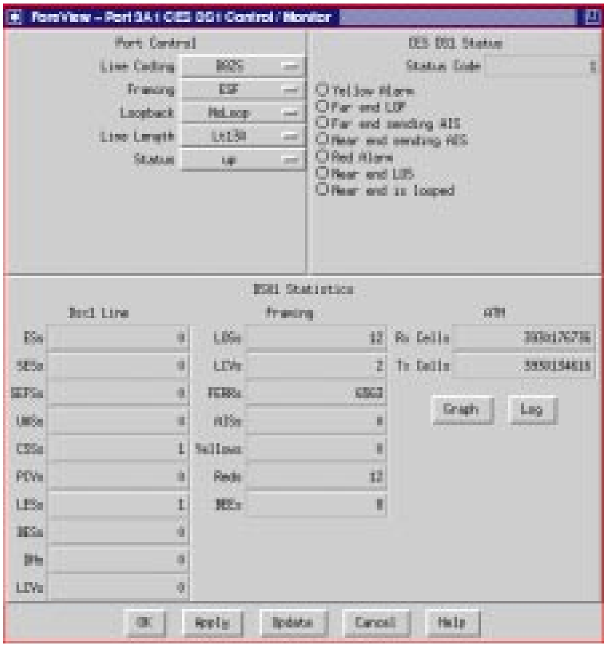
HCSs Indicates the number of header check sequence (HCS) error events. The HCS is a CRC-8 calculation over the first 4 octets of the ATM cell header.

Rx Cells Displays the number of ATM cells that were received.

Tx Cells Shows the number of ATM cells that were transmitted.

8.17 Configuring and Monitoring CEMDS1 Ports

To configure, check the status of, and view statistics for CES-DS1 ports, select the CES-DS1 port(s) from a front panel, pull down the **`Configure/Port`** menu and launch the CES-DS1 Control/Monitor dialog. The CES-DS1 Control/Monitor dialog is shown in the following figure:



ForeView - Port 3A1 CES DS1 Control / Monitor

Port Control

Line Coding: B8ZS
Framing: ESF
Loopback: NoLoop
Line Length: Lt150
Status: up

CES DS1 Status

Status Code: 1

○ Yellow Alarm
○ Far end LOF
○ Far end sending AIS
○ Near end sending AIS
○ Red Alarm
○ Near end LOS
○ Near end is looped

DS1 Statistics

Dsx1 Line		Framing		ATM	
ESs	0	LOSs	12	Rx Cells	3930176736
SESs	0	LCVs	2	Tx Cells	3930194618
SEFSs	0	FEBEs	6863		
UASs	0	AISs	0		
CSSs	1	Yellows	0		
PCVs	0	Reds	12		
LESs	1	BEEs	0		
BESs	0				
DMs	0				
LCVs	0				

Figure 8.17 - CES-DS1 Control/Monitor Dialog

8.17.1 CEMDS1 Port Control

The fields in this section of the display are defined as follows:

Line Coding Selects the type of coding to be used. B8ZS indicates that Binary 8-Zero Substitution will be used. AMI indicates that Alternate Mark Inversion will be used.

Framing Selects the type of framing on the port. ESF indicates that ESF (Extended Super Frame) framing will be used. SF indicates that SF (Super Frame) framing will be used.

Loopback Selects the loopback setting on the port. Setting `Line` loopback connects the transmitter to the receiver. The data stream received from the Rx line is retransmitted out to the Tx line. Cells that are switched to this port are not sent over the line. Selecting `NoLoop` designates that no loopback will take place. This is the default setting.

Line Length Selects the line length of a CESDS1 port to correspond to the physical cable attached to that port. This lets the CESDS1 port anticipate the strength of the received signal on the cable. Options are: Lt130, which indicates that the physical cable is shorter than 130 feet long (<40m); 130-260, which indicates that the physical cable is from 130 to 260 feet long (40-80m); 260-390, which indicates that the physical cable is from 260 to 390 feet long (80-120m); or 390, which indicates that the physical cable is greater than 390 feet long (>120m).

Status Indicates the CESDS1 line status of the port, up or down.

8.17.2 CEMDS1 Status

Yellow Alarm Indicates that Yellow Alarm events have been detected.

Far end LOF Indicates whether or not the port is receiving a Loss of Frame (LOF) signal from the far end.

Far end sending AIS Indicates whether or not the port is receiving an Alarm Indication Signal (AIS) from the far end.

Near end sending AIS Indicates whether or not the port is transmitting an Alarm Indication Signal (AIS) from the near end.

Red Alarm Indicates that Red Alarm events have been detected.

Near end LOS Indicates whether or not the port is experiencing a Loss of Signal (LOS) from the near end.

Near end is looped Indicates whether or not the port is in loopback mode.

8.17.3 CEMDS1 Statistics

8.17.3.1 DSx1 Line

ESs Shows the number of Errored Seconds seen on the port.

SESs Shows the number of Severely Errored Seconds seen on the port.

EFSs

UASs Shows the number of Unavailable Seconds seen on the port.

CSSs Shows the number of Controlled Slip Seconds seen on the port.

PCVs Shows the number of Path Coding Violations seen on the port.

LESs Shows the number of Line Errored Seconds seen on the port.

BESs Shows the number of Bursty Errored Seconds seen on the port.

DMs Shows the number of Degraded Minutes seen on the port.

LCVs Shows the number of Line Coding Violations seen on the port.

8.17.3.2 Framing

LOSs Shows the number of seconds in which Loss Of Signal (LOS) errors have been detected.

LCVs Shows the number of Line Code Violations (LCV) that have been detected.

FERRs Shows the number of DS1 framing error (FERR) events that have been detected.

AISs Shows the number of seconds in which Alarm Indication Signals (AIS) were detected by the DS1 Receive Framer block. AIS indicates that an upstream failure has been detected by the far end.

Yellows Shows the number of seconds in which Yellow Alarm events have been detected.

Reds Shows the number of seconds in which Red Alarm events have been detected.

BEEs Shows the number of Bit Encoding Error (BEE) events that have been detected.

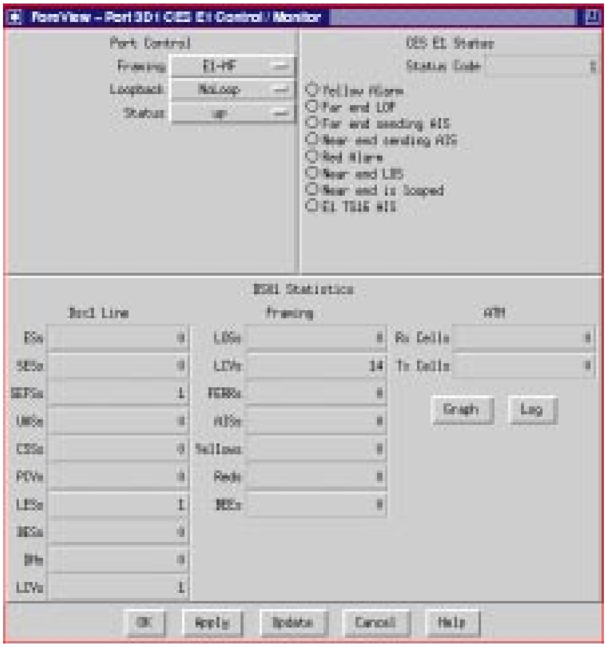
8.17.3.3 ATM

Rx Cells Shows the number of ATM cells that were received, not including idle/unassigned cells.

Tx Cells Shows the number of ATM cells that were transmitted, not including idle/unassigned cells.

8.18 Configuring and Monitoring CEME1 Ports

To configure, check the status of, and view statistics for CES-E1 ports, select the CES-E1 port(s) from a front panel, pull down the **`Configure/Port`** menu and launch the CES-E1 Control / Monitor dialog. The CES-E1 Control / Monitor dialog is shown in the following figure:



ForeView – Port 3D1 CES E1 Control / Monitor

Port Control

Framing: E1-MF

Loopback: NoLoop

Status: up

CES E1 Status

Status Code: 1

○ Yellow Alarm
○ Far end LOF
○ Far end sending AIS
○ Near end sending AIS
○ Red Alarm
○ Near end LOS
○ Near end is looped
○ E1 TS16 AIS

DSX1 Statistics

Dsx1 Line		Framing		ATM	
ESs	0	LOSs	0	Rx Cells	0
SESs	0	LCVs	14	Tx Cells	0
SEFSs	1	FERRs	0		
UASs	0	AISs	0		
CSSs	0	Yellows	0		
PCVs	0	Reds	0		
LESs	1	BEEs	0		
BESs	0				
DMs	0				
LCVs	1				

Figure 8.18 - CES-E1 Control / Monitor Dialog

8.18.1 CEME1 Port Control

The fields in this section of the display are defined as follows:

Framing Selects the type of framing on the port. E1 indicates that basic E1 framing is used. CRC indicates that E1 framing with CRC-4 checksums is used. MF indicates that multiframe E1 framing is used. CRCMF indicates that multiframe E1 framing with CRC-4 checksums is used.

Loopback Selects the loopback setting on the port. Setting `Line` loopback connects the transmitter to the receiver. The data stream received from the Rx line is retransmitted out to the Tx line. Cells that are switched to this port are not sent over the line. Selecting `NoLoop` designates that no loopback will take place. This is the default setting.

Status Indicates the CESDS1 line status of the port, up or down.

8.18.2 CEME1 Status

Yellow Alarm Indicates that Yellow Alarm events have been detected.

Far end LOF Indicates whether or not the port is receiving a Loss of Frame (LOF) signal from the far end.

Far end sending AIS Indicates whether or not the port is receiving an Alarm Indication Signal (AIS) from the far end.

Near end sending AIS Indicates whether or not the port is transmitting an Alarm Indication Signal (AIS) from the near end.

Red Alarm Indicates that Red Alarm events have been detected.

Near end LOS Indicates whether or not the port is experiencing a Loss of Signal (LOS) from the near end.

Near end is looped Indicates whether or not the port is in loopback mode.

E1 TS16 AIS Indicates whether AIS is being received in timeslot 16.

8.18.3 CEME1 Statistics

8.18.3.1 E1 Line

ESs Shows the number of Errored Seconds seen on the port.

SESs Shows the number of Severely Errored Seconds seen on the port.

EFSs

UASs Shows the number of Unavailable Seconds seen on the port.

CSSs Shows the number of Controlled Slip Seconds seen on the port.

PCVs Shows the number of Path Coding Violations seen on the port.

LESs Shows the number of Line Errored Seconds seen on the port.

BESs Shows the number of Bursty Errored Seconds seen on the port.

DMs Shows the number of Degraded Minutes seen on the port.

LCVs Shows the number of Line Coding Violations seen on the port.

8.18.3.2 Framing

LOSs Shows the number of seconds in which Loss Of Signal (LOS) errors have been detected.

LCVs Shows the number of Line Code Violations (LCV) that have been detected.

FERRs Shows the number of DS1 framing error (FERR) events that have been detected.

AISs Shows the number of seconds in which Alarm Indication Signals (AIS) were detected by the DS1 Receive Framer block. AIS indicates that an upstream failure has been detected by the far end.

Yellows Shows the number of seconds in which Yellow Alarm events have been detected.

Reds Shows the number of seconds in which Red Alarm events have been detected.

BEEs Shows the number of Bit Encoding Error (BEE) events that have been detected.

8.18.3.3 ATM

Rx Cells Shows the number of ATM cells that were received, not including idle/unassigned cells.

Tx Cells Shows the number of ATM cells that were transmitted, not including idle/unassigned cells.

8.19 Configuring Port Level Traffic

In accordance with the UNI 3.x specification for traffic policing, a *ForeRunner* switch ensures that the traffic on an ATM connection remains within the negotiated contract between the user and the network. While performing the policing, if the contract is violated, the switch has the option of either discarding non-conforming ATM cells or tagging them as non-conforming by setting the Cell Loss Priority (CLP) bit to 1 in the ATM cell header.

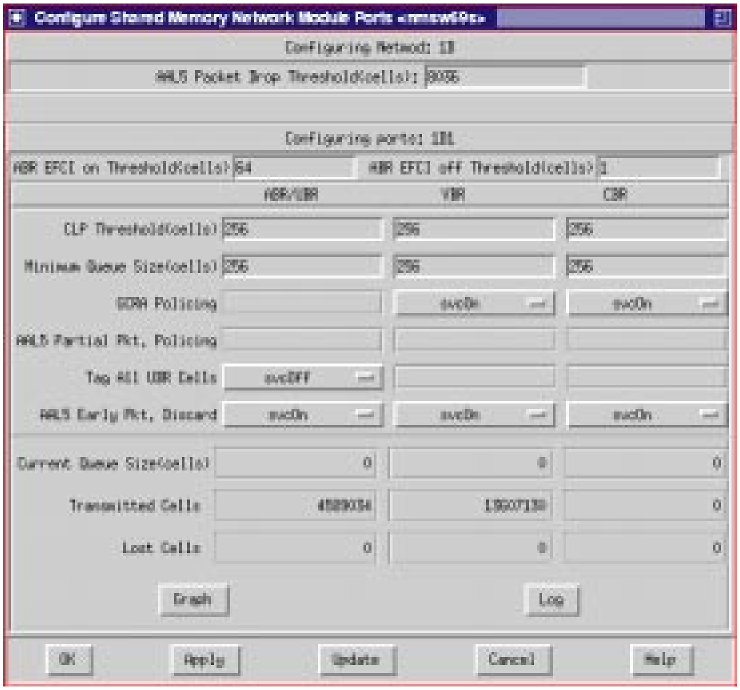
This menu option allows you to configure various traffic features on an individual port on a Series C or Series LC network module on the switch. You can reach this level by selecting a port or ports and then by pulling down the **`Configure/Port/Traffic`** menu.

8.19.1 Series D Network Modules

This release of *ForeView* provides limited support for FORE's Series D network modules. The Series D network modules will be identified on a switch front panel, and those Series D features common to Series C and LC network modules are supported. Full Series D support, when available, will include: CLP thresholds, connection scheduling, extended traffic statistics for graphing and logging, and enhanced memory models.

8.19.2 Series C Network Modules

To configure various traffic management features on an individual port on a Series C network module on the switch, select a port and then pull down the **`Configure/Port/Traffic`** menu.



Configure Shared Memory Network Module Ports <nmsw69c>

Configuring Netmod: 1B

AAL5 Packet Drop Threshold(cells): 8036

Configuring ports: 1B1

ABR EFCI on Threshold(cells) 64

ABR EFCI off Threshold(cells) 1

	ABR/UBR	VBR	CBR
CLP Threshold(cells)	256	256	256
Minimum Queue Size(cells)	256	256	256
GCRA Policing		svcOn	svcOn
AAL5 Partial Pkt, Policing			
Tag All UBR Cells	svcOFF		
AAL5 Early Pkt, Discard	svcOn	svcOn	svcOn
Current Queue Size(cells)	0	0	0
Transmitted Cells	4589034	13907138	0
Lost Cells	0	0	0

Figure 8.19 - Port Traffic Dialog for Series C Network Modules

The fields are defined as follows:

AAL 5 Packet Drop Threshold(cells) Indicates the number of cells in the buffer at which the specified traffic type drops CLP=1 cells. The default is 256 cells.

ABR EFCI on Threshold(cells) Indicates the number of cells over which the ABR cells will have EFCI set. The default value is 64 cells. The EFCI is set when the threshold number is reached, signalling congestion.

ABR EFCI off Threshold(cells) Indicates the number of cells reached which the will disable EFCI. The default value is 1 cell. The EFCI is cleared when the threshold number is reached, indicating no congestion.

CLP Threshold The Cell Loss Priority (CLP) threshold for ABR/UBR, VBR, and CBR traffic. This is the value at which cells that have been tagged as non-conforming are dropped for this port and priority. The default is 256 cells for each traffic type. This parameter can not be changed.

Minimum Queue Size Enables you to designate the minimum queue size for a given type of traffic on a specified port on a Series C network module. The default is 256 cells.

GCRA Policing Generic Cell Rate Algorithm (GCRA) policing ensures that traffic is regulated at the ATM layer on the input side of the network. This option allows you to configure GCRA policing on a per-port/per-class basis for all CBR and/or VBR PVCs and/or SVCs.

AAL5 Partial Pkt. Policing This option lets you configure partial packet policing on a per-port/per-class basis for all CBR and/or VBR PVCs and/or SVCs. When partial packet policing is enabled on a connection, the GCRA policer looks for AAL5 packet boundaries by checking for cells with an EOM indicator in their cell header. If the policer decides that a cell in the middle of the AAL5 packet is non-conforming, then all remaining cells in that AAL5 packet (up to, but not including the EOM cell) are considered non-conforming.

Tag All UBR Cells The Tag All UBR Cells menu button is to either enable or disable tagging of all UBR traffic cells. The default value is ‘no Tagging’.

AAL5 Early Packet Discard The AAL5 Early Packet Discard menu button is to either enable or disable the early packet discard functionality for egress AAL5 traffic cells. This button is active only if the connection is an AAL5 connection. The default value is ‘enabled’.

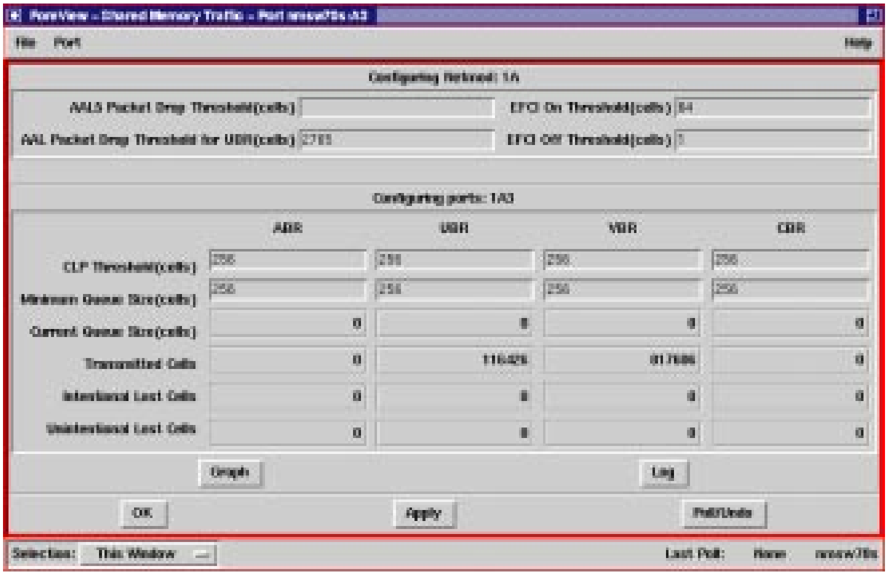
Current Queue Size The queue size in cells for ABR/UBR, VBR, and CBR traffic. The default is 256 cells for each traffic type.

Transmitted Cells Displays the number of non-null ATM cells that were transmitted for ABR/UBR, VBR, and CBR traffic.

Lost Cells Displays the number of ATM cells that were lost or dropped for ABR/UBR, VBR, and CBR traffic.

8.19.3 Series LC Network Modules

To configure various traffic management features on an individual port on a Series LC network module on the switch, select a port and then pull down the **`Configure/Port/Traffic`** menu.



Configuring Netmod: 1A

AAL5 Packet Drop Threshold(cells)		EFCI On Threshold(cells)	64
AAL Packet Drop Threshold for UBR(cells)	2785	EFCI Off Threshold(cells)	1

Configuring ports: 1A3

	ABR	UBR	VBR	CBR
CLP Threshold(cells)	256	256	256	256
Minimum Queue Size(cells)	256	256	256	256
Current Queue Size(cells)	0	0	0	0
Transmitted Cells	0	116426	817686	0
Interleaved Lost Cells	0	0	0	0
Uninterleaved Lost Cells	0	0	0	0

Selection: This Window   Last Poll: None

Figure 8.20 - Port Traffic Dialog for LC Network Modules

The options are defined as follows:

AAL5 Packet Drop Threshold (cells) This option shows the AAL5 packet drop threshold for CBR, VBR, and ABR traffic, in cells, on this network module.

AAL5 Packet Drop Threshold for UBR (cells) This option shows the AAL5 packet drop threshold for UBR traffic, in cells, on this network module.

EFCI On Threshold (cells) This option shows the threshold value at which the EFCI will be set (turned on), signalling congestion, for ABR traffic.

EFCI Off Threshold (cells) This option shows the threshold value at which the EFCI will be cleared (turned off), indicating no congestion for ABR traffic.

NOTE

The value for the off threshold must always be less than the value for the on threshold.

CLP Threshold (cells) This option lets you designate the CLP=1 threshold at which cells that have been tagged as non-conforming are dropped for a given traffic type on a specified port on a Series LE network module. The default is 256 cells for the type of traffic (ABR, UBR, VBR, or CBR) the CLP threshold is being set.

Minimum Queue Size (cells) Specifies the queue size to be assigned to the traffic designated in the previous parameter. The default is 256 cells for the type of traffic (ABR, UBR, VBR, or CBR) the queue size is being set.

The following are read-only counters for each type of traffic (ABR, UBR, VBR, or CBR).

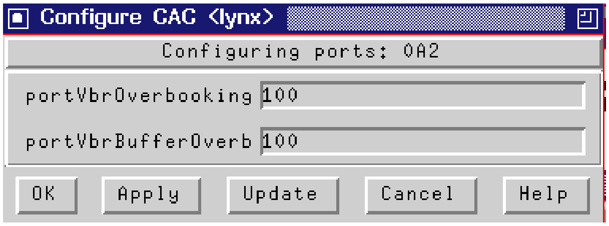
Transmitted Cells Shows the number of cells transmitted for the selected port.

Intentional Lost Cells Shows the number of intentional cells lost for the selected port.

Unintentional Lost Cells Shows the number of unintentional cells lost for the selected port.

8.20 Configuring Port Level CAC

The port-level CAC (Connection Admission Control) option allows you to set an output bandwidth overbooking level and an output buffer overbooking level for VBR traffic on a particular port.



Configuring ports: 0A2

portVbrOverbooking 100

portVbrBufferOverb 100

Figure 8.21 - Overbooking CAC Dialog

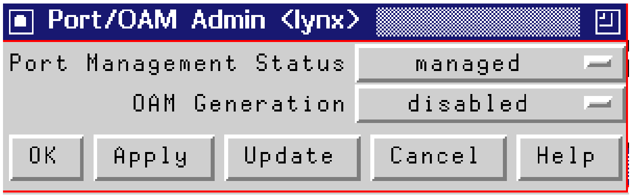
The fields in this dialog are defined as follows:

portVbrOverbooking For the selected port, indicates the bandwidth overbooking level assigned to this port, specified as a percentage. Enter an integer value from 1 to 500. The default is 100, which indicates that no overbooking will occur. Values less than 100 cause underbooking. Values greater than 100 denote overbooking.

portVbrBufferOverb For the selected port, indicates the buffer overbooking level assigned to this port, specified as a percentage. Enter an integer value greater than or equal to 1. The default is 100, which means that no overbooking has been defined. Values less than 100 cause underbooking. Values greater than 100 denote overbooking.

8.21 OAM Management

The *ForeView* user interface allows network managers to activate or deactivate OAM cell generation on a port-by-port basis in FORE ATM switches supporting OAM. From a *ForeView* front panel, pull down the **`Configure`** menu and select **`Port -> Port/OAM Admin`**. This launches the per-port OAM administration dialog, as illustrated below.



Port/OAM Admin <lynx>

Port Management Status: managed

OAM Generation: disabled

Figure 8.22 - OAM Administration Dialog

The dialog options are defined as follows:

Port Management Status Defines the port status, either managed or unmanaged.

OAM Generation Indicates whether OAM cell generation is enabled or disabled for the selected port(s). When a user toggles the OAM Generation, an SNMP command is sent to the switch to activate/deactivate OAM cell generation on the selected port(s). Once enabled, (F4/F5 AIS and F4 RDI) cells (whichever is applicable) will be generated on the port(s) whenever valid conditions exist. Transmitted OAM cells will be counted, and time stamp maintained on the generating switch.

NOTE This dialog does not affect the switch's ability to receive, time stamp and count incoming OAM cells. Port/OAM administration will be disabled on a FORE ATM switch not supporting OAM.

8.22 Configuring and Monitoring Network Modules

The Module menu lets you configure the network modules. You can reach this level by selecting **`Configure/Module`** from a front panel. The menu also allows you to find information about shared memory network modules.

The following choices are available:

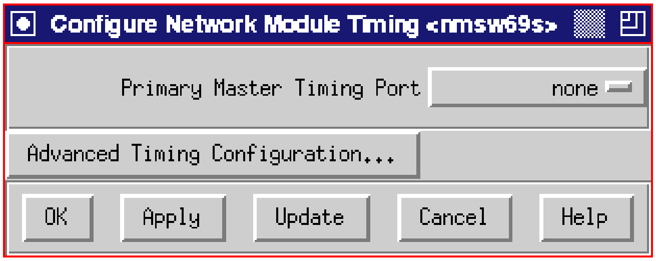
Traffic Allows you to select the AAL 5 packet drop threshold on a network modules and find information about traffic on shared memory network modules. See Section 8.19 for an example of the dialogs for traffic configuration.

8.23 Configuring Timing

Select **`Configure/Timing`** to configure or to display information about the timing source of the network modules. This launches the Configure Network Module Timing dialog, as illustrated below.

NOTE

This configuration dialog applies only to FORE Systems' Series LC network modules and to Series C network modules that have distributed timing support. On an LE 155 switch, interface D1 is the only one that can export a timing source.


Configure Network Module Timing <nmsw69s>

Primary Master Timing Port: none

Figure 8.23 - Timing Configuration Dialog

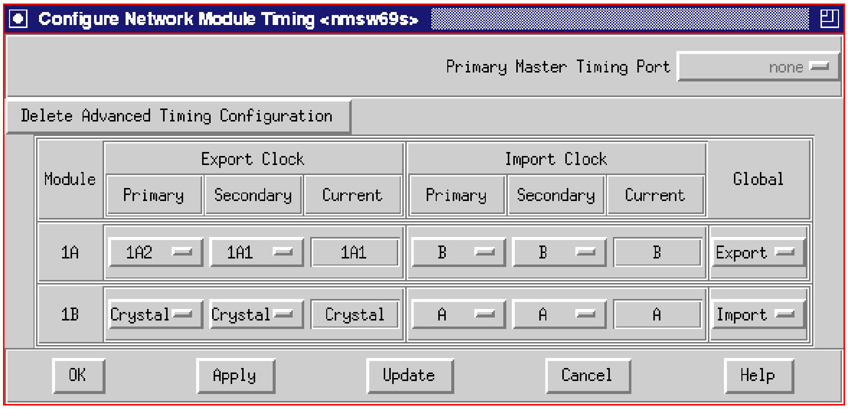
The dialog options are defined as follows:

Primary Master Timing Port Select the preferred export timing source for the selected network module interface. This clock source may be retrieved either from one of the ports on this network module via the pull-down, or from the crystal oscillator on this network module.

Advanced Timing Configuration... Expand the dialog to perform advanced timing configurations.

8.23.1 Advanced Timing

Select the **`Advanced Timing Configuration...`** to configure or to display advanced level information about the timing source of the network modules. This expands the Configure Network Module Timing dialog, as illustrated below.


Configure Network Module Timing <nmsw69s>
Delete Advanced Timing Configuration
OK
Apply
Update
Cancel
Help

Primary Master Timing Port: none

Module	Export Clock			Import Clock			Global
	Primary	Secondary	Current	Primary	Secondary	Current	
1A	1A2	1A1	1A1	B	B	B	Export
1B	Crystal	Crystal	Crystal	A	A	A	Import

Figure 8.24 - Advanced Timing Configuration Dialog

The dialog options are defined as follows:

Module

Indicates the specific distributed timing network module to be configured.

Primary or Secondary (Export)

Using `primary` designates this as the preferred export timing source for this network module. Using `secondary` designates this as the backup export timing source to be used for this network module in the event that the primary source is unavailable.

Using `port#` means that the timing source is recovered externally from this specific port on a distributed timing network module. Using `crystal` means that the timing is derived internally from the crystal oscillator on this network module. `None` is only available on the TP25 network module. Using `none` allows the TP25 network module to disable transmitting sync pulses.

Primary or Secondary (Import)

Using `primary` designates this as the preferred import timing source for this network module. Using `secondary` designates this as the backup import source to be used for this network module in the event that the primary source is unavailable.

The imported clock may be used as the network module global clock, which in turn, may be used by all ports that link their transmit clock to the network module global clock. Can be from the export clock from another (`A` - bottom left, `B` - bottom right, `C` - top left, or `D` - top right) network module on this switch fabric, or the export clock from another (1 - first (leftmost slot), 2 - second slot, 3 - third slot, 4 fourth slot) switch fabric.

NOTE

You cannot import the clock from the fabric you are currently using; i.e., if you are configuring board 2, you cannot use 2 as the value for `(A|B|C|D|1|2|3|4)`.

8.24 Configuring IP

The **`Configure`** option of the Front Panel provides the following choices:

Port This menu allows you to configure ports, view statistics, and configure port-specific shared memory options.

Module This menu allows you to configure network module timing and traffic (shared memory).

IP This menu allows you to modify the IP address of the switch’s IP interfaces.

Signalling This menu allows you to create signalling paths for SPANS and UNI 3.x protocols.

Alarms This menu allows you to view the state of and change the priority of alarm types related to ASX-200BX and ASX-200BXE switches.

NSAP This menu allows you to configure NSAP prefixes and addresses.

UPC This menu allows you to configure the Usage Parameter Control (UPC) contracts that establish quality of service for VCCs. See Chapter 9.

AVR Configures the Address Validation threshold.

PMP Configures the Point-to-Multipoint minimum and maximum VCI allocation.

PNNI-SPVC Configures Pacing and Rerouting parameters for the PNNI SPVCs.

The **`IP`** menu option allows you to change the IP configurations. You can reach this level by selecting **`Configure/IP`** from the Front Panel.

The following choices are available:

Interfaces This menu allows you to modify the IP address of the switch’s IP interfaces.

Routes This menu allows you to modify the IP routes of the switch’s IP interfaces.

8.25 Configuring IP Interfaces

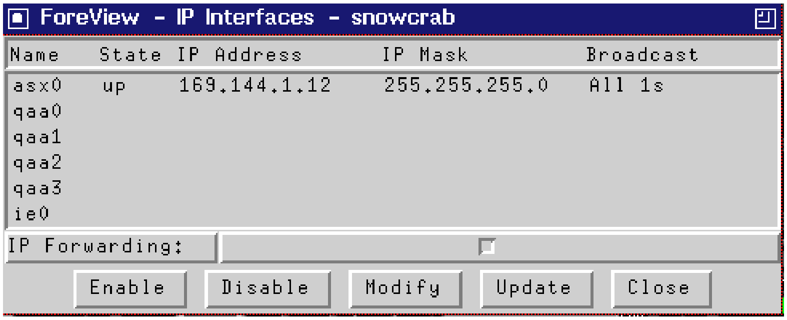
This menu allows you to configure or modify the IP address of the switch's IP interfaces. You can reach this level by selecting a port or ports and then by pulling down the **Configure/IP** menu.

NOTE

On a new switch, the **ie0** (**le0** on an ASX-200), **asx0**, **qaa0**, **qaa1**, **qaa2**, **qaa3** interfaces are NOT configured. An IP address must be configured for at least one of the interfaces to allow IP access to the switch, which, in turn, enables SNMP access. By setting the IP address of the **asx0** interface or one of the **qaa** interfaces, in-band (over ATM) access to the switch control processor (SCP) is enabled. By setting the IP address of the **ie0** (**le0** on an ASX-200) interface, out-of-band access to the SCP is enabled.

NOTE

The IP addresses must be configured individually on each SCP on an ASX-1000.



Name	State	IP Address	IP Mask	Broadcast
asx0	up	169.144.1.12	255.255.255.0	All 1s
qaa0				
qaa1				
qaa2				
qaa3				
ie0				

IP Forwarding: □

Figure 8.25 - IP Interfaces Dialog

The fields are defined as follows:

Name Indicates the name of the IP interface to be managed. Valid interfaces are: **`ie0`** (the Ethernet interface) (**`le0`** on an ASX-200), **`asx0`** (the switch's SPANS interface), **`qaa0`**, **`qaa1`**, **`qaa2`**, **`qaa3`** (the Classical IP interfaces). The state of the interface must be up before setting or modifying the address.

State Indicates the state of the corresponding interface, either **up** or **down**. The state of the interface must be **up** before setting or modifying the address.

IP Address Shows the IP address of the IP interface.

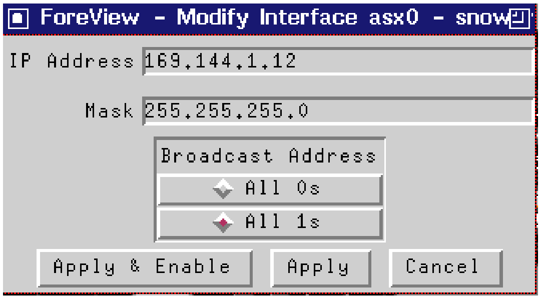
IP Mask Indicates the subnet mask for this IP interface.

Broadcast Indicates the IP broadcast type for this interface, either all 0s or all 1s. This is the host portion of the IP address that is used for routing.

IP Forwarding This toggle allows you to turn IP forwarding on or off. If IP forwarding is turned off, the switch will not forward (i.e., route) IP packets from one IP interface to another IP interface. It is generally not necessary to turn IP forwarding off, except for security reasons.

8.25.1 Modifying an IP Interface

Place the cursor on any of the IP interface names and click on the **`Modify`** button to edit any of the IP interface types.



ForeView - Modify Interface asx0 - snow

IP Address 169.144.1.12

Mask 255.255.255.0

Broadcast Address

○ All 0s

● All 1s

Figure 8.26 - Modify IP Interface Dialog

The following modifications are available:

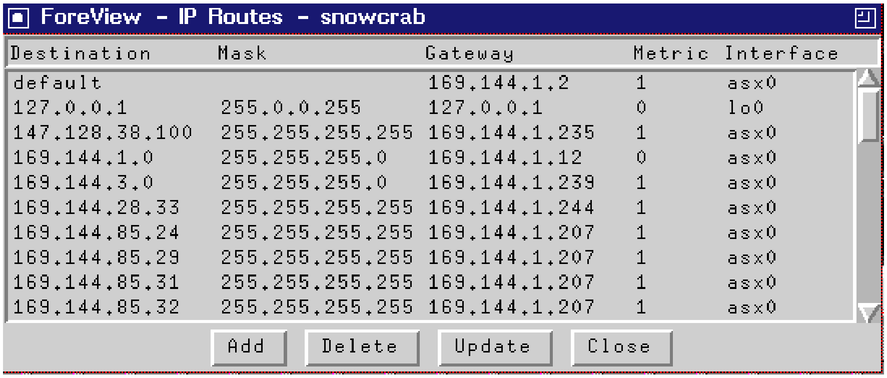
IP Address Enter an IP address for the selected IP interface.

Mask Enter a subnet mask for this IP interface.

Broadcast Address Select the IP broadcast type for this interface, either All 0s or All 1s. This is the host portion of the IP address that is used for routing.

8.26 Configuring IP Routing

This menu allows you to configure or to modify IP routes. You can reach this level by selecting a port or ports and then by pulling down the **`Configure/IP`** menu.



Destination	Mask	Gateway	Metric	Interface
default		169.144.1.2	1	asx0
127.0.0.1	255.0.0.255	127.0.0.1	0	lo0
147.128.38.100	255.255.255.255	169.144.1.235	1	asx0
169.144.1.0	255.255.255.0	169.144.1.12	0	asx0
169.144.3.0	255.255.255.0	169.144.1.239	1	asx0
169.144.28.33	255.255.255.255	169.144.1.244	1	asx0
169.144.85.24	255.255.255.255	169.144.1.207	1	asx0
169.144.85.29	255.255.255.255	169.144.1.207	1	asx0
169.144.85.31	255.255.255.255	169.144.1.207	1	asx0
169.144.85.32	255.255.255.255	169.144.1.207	1	asx0

Figure 8.27 - IP Routing Dialog

The fields are defined as follows:

Destination Indicates the destination IP network address.

Mask Indicates the subnet mask for the destination IP interface.

Gateway Indicates the gateway address to the destination IP network number.

Metric Indicates the number of hops to the destination IP network.

Interface Indicates the local IP interface type used to get to the destination IP network. Valid interfaces are: le0, asx0, qaa0, qaa1, qaa2, and qaa3.

8.26.1 Adding an IP Route

Click on the **Add** button to create an IP route.

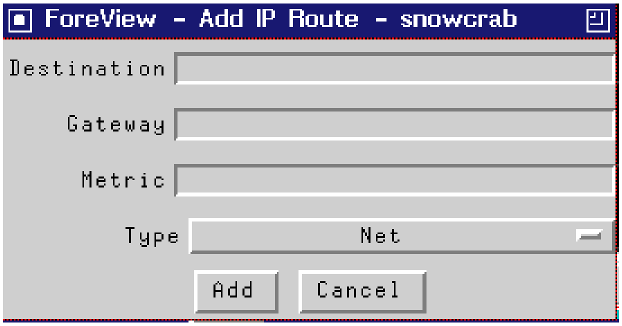


Figure 8.28 - Add an IP Route Dialog

The following entries are required to add an IP route:

Destination Enter an IP address for the destination.

Gateway Enter the gateway address to the destination IP network number.

Metric Enter the number of hops to the destination IP network.

Type This toggle allows you to select the type of IP route. Using **host** indicates that this is a host-specific route with the destination being a specific node's IP address. Using **net** indicates that this is a network-specific route with the destination being a network IP address. The default is **net**.

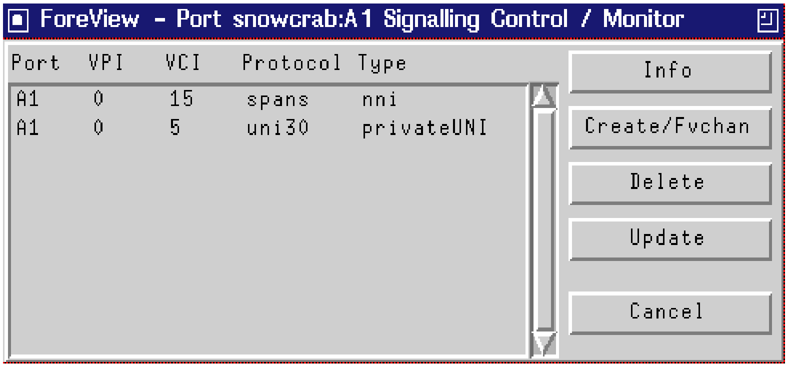
8.27 Configuring Signalling

The **`Signalling`** menu option allows you to view the signalling paths that exist on selected ports. You can also create signalling paths by selecting **`Create/Fvchan`**, which launches the Virtual Path / Channel Tool.

NOTE

Please refer to Chapter 9 for information on creating signalling paths using SPANS, FORE Systems' proprietary signaling protocol, or UNI 3.x signalling.

You can reach this level by selecting a port or ports and then by pulling down the **`Configure/Signalling`** from a front panel. From this dialog, view information about signalling paths by selecting **`Info`**, create paths by selecting **`Create/Fvchan`**, and delete paths using the **`Delete`** function.



```
Port   VPI   VCI   Protocol  Type
A1     0     15    spans     nni
A1     0     5     uni30     privateUNI
```

Figure 8.29 - Signalling Control Dialog

The fields are defined as follows:

Port Indicates the port number on which the signaling path is being monitored.

VPI This is the number of the path for a corresponding signal / port.

VCI This is the number of the channel for a corresponding signal / port.

Protocol Indicates the type of protocol in use for this signaling path, either SPANS or UNI 3.x.

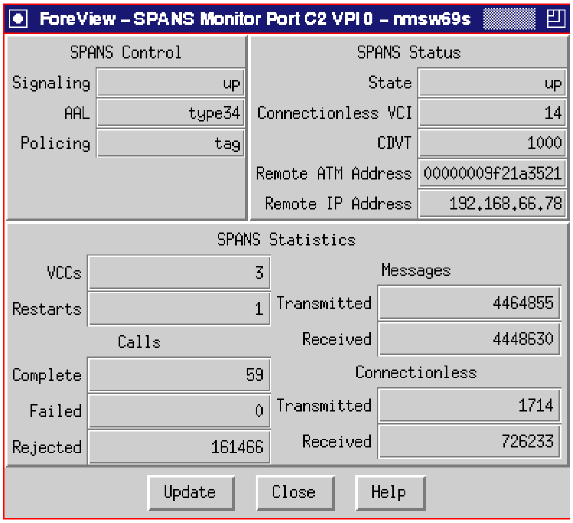
Type Designates the type of connection on this path. If the type listed is uni, then this is a user-to-network interface connection to a host. If the type listed is nni, then this is a network-to-network interface connection to another switch.

8.27.1 Signalling Information

The **`Signalling`** dialog provides a method to view information about signalling paths. Select a signalling path (either SPANS or UNI 3.x) and then select **`Info`**, which launches an information dialog for the the type of path selected.

8.27.1.1 SPANS Information

Select a SPANS signalling path and then select **`Info`** to launch the following information dialog.



ForeView – SPANS Monitor Port C2 VPI 0 – nmsw69s

SPANS Control
Signaling: up
AAL: type34
Policing: tag

SPANS Status
State: up
Connectionless VCI: 14
CDVT: 1000
Remote ATM Address: 00000009f21a3521
Remote IP Address: 192.168.66.78

SPANS Statistics
VCCs: 3
Restarts: 1

Calls
Complete: 59
Failed: 0
Rejected: 161466

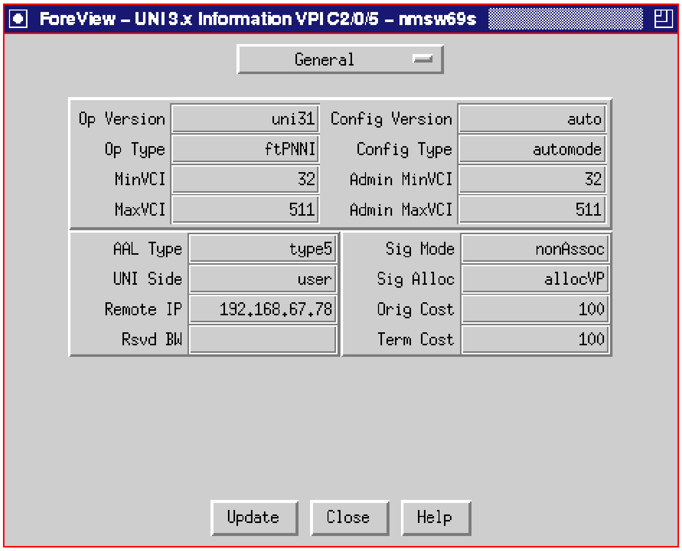
Messages
Transmitted: 4464855
Received: 4448630

Connectionless
Transmitted: 1714
Received: 726233

Figure 8.30 - SPANS Information Dialog

8.27.1.2 UNI 3.x Information

Select a UNI 3.x signalling path and then select **Info** to launch the following information dialog. This selection defaults to the **General** UNI 3.x information dialog. Three other information options are available from pull-down menu: **Status & Statistics**, **ILMI**, and **E164 & AV**.



ForeView – UNI 3.x Information VPI C2/0/5 – nmsw69s

General

Op Version	uni31	Config Version	auto
Op Type	ftPNNI	Config Type	automode
MinVCI	32	Admin MinVCI	32
MaxVCI	511	Admin MaxVCI	511
AAL Type	type5	Sig Mode	nonAssoc
UNI Side	user	Sig Alloc	allocVP
Remote IP	192.168.67.78	Orig Cost	100
Rsvd BW		Term Cost	100

Figure 8.31 - UNI 3.x Information Dialog

8.28 Alarm Control

The *ForeRunner* switches will report alarm conditions to *ForeView*. The **Link Failed** and **Signaling Failed** alarms are available on all *ForeRunner* switches. The **Input Power Failure** and **Over Temperature** alarms are available on all switches, except the ASX-200 and the LE-155. The **Output Power Failure** alarm is available only on the ASX-200BX, the ASX-200WG, and the ASX-1000. The **Fan Bank Failed** alarm is available only on the ASX-200BX, the ASX-200WG, and the ASX-1000. The **Over Current** and **5 Volt Failure** alarms are applicable to switches configured with 30 amp DC power supplies.

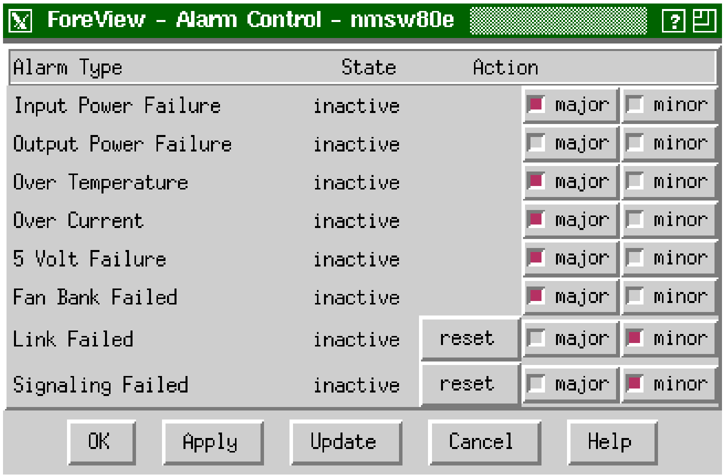
In the ASX-1000, a built-in thermal temperature sensor resides on each switch board and reads out the board's local temperature. By default, the switch control software will trigger an alarm at 65°C and will reset the alarm when the temperature drops back down to 60°C or lower. However, you can configure alarm and reset thresholds in the software on an individual board via AMI. Please refer to the *ForeRunner* ATM Switch Configuration Manual for more information about configuring these thresholds. If the temperature of an individual switch board were to reach 75°C, the switch board would shut itself down immediately.

CAUTION

Upon detection of an overtemperature condition, the ASX-1000 should be turned off to avoid damage to internal components.

The Common Equipment Card (CEC) provided with the ASX-1000 is responsible for monitoring the environmental conditions of the switch and reporting this information to the switch control processors. The CEC reports conditions such as malfunctioning fans, overheated power supplies, and an overheated enclosure.

To view the state of Alarm Control, select **Alarms** from the **Configure** pull-down menu of a Front Panel display. A dialog similar to the figure below will appear. From this dialog, view the Alarm Type, the state of individual alarm conditions, and the Action of each alarm condition (major or minor).



Alarm Type	State	Action		
Input Power Failure	inactive		☒ major	□ minor
Output Power Failure	inactive		□ major	□ minor
Over Temperature	inactive		☒ major	□ minor
Over Current	inactive		☒ major	□ minor
5 Volt Failure	inactive		☒ major	□ minor
Fan Bank Failed	inactive		☒ major	□ minor
Link Failed	inactive	reset	□ major	☒ minor
Signaling Failed	inactive	reset	□ major	☒ minor

Figure 8.32 - Alarm Control Dialog

The fields in this display have the following meanings:

Alarm Type Displays the name of the alarm.

State Shows whether the state of the alarm is active (alarming) or inactive (not alarming). An alarm is active if the underlying condition is detected. For power supplies, the input failed alarm condition is active if the input voltage is not within the nominal range for the supply. This does not necessarily mean that an output failure will result. A power supply output failure condition is active if any power supply is failing or if it is physically removed.

Action Selection that determines how the alarm is classified. **major** means that this alarm type will cause a major alarm. **minor** means that this alarm type will cause a minor alarm.

Reset Allows you to reset either the **Link Failed** alarm, the **Signaling Failed** alarm, or both alarms.

8.29 Configuring ATM Connection Routing

The **Configure** option of the Front Panel provides the following choices:

Port This menu allows you to configure ports, view statistics, and configure port-specific shared memory options.

Module This menu allows you to configure network module timing and traffic (shared memory).

IP This menu allows you to modify the IP address of the switch's IP interfaces.

Signalling This menu allows you to create signalling paths for SPANS and UNI 3.x protocols.

Alarms This menu allows you to view the state of and change the priority of alarm types related to ASX-200BX and ASX-200BXE switches.

NSAP This menu allows you to configure NSAP prefixes and addresses.

UPC This menu allows you to configure the Usage Parameter Control (UPC) contracts that establish quality of service for VCCs. See Chapter 9.

AVR Configures the Address Validation threshold.

PMP Configures the Point-to-Multipoint minimum and maximum VCI allocation.

PNNI-SPVC Configures Pacing and Rerouting parameters for the PNNI SPVCs.

8.30 Configuring NSAP Routing

This menu option allows you to create, delete, and display routes to NSAP addresses and to create, delete, and display NSAP prefixes. You can reach this level by selecting a port or ports and then by pulling down the **`Configure/NSAP`** menu.

The following choices are available:

Prefixes This menu lets you create, delete, and display prefixes to NSAP addresses.

Static Routing This menu lets you create, delete, and display static routes to NSAP addresses.

Show ILMI This option lets you view the NSAP addresses that are registered by ILMI.

8.30.1 Prefixes

This menu option allows you to delete an NSAP prefix, create an NSAP prefix, and display NSAP prefix information. You can reach this level by selecting a port or ports and then by pulling down the **`Configure/NSAP`** menu.

The following choices are available:

ICD This menu configures NSAP prefixes requiring the International Code Designator (ICD). An ICD identifies an international organization.

DCC This menu configures NSAP prefixes requiring the Data Country Code (DCC). A DCC specifies the country in which an address is registered.

E.164 This menu configures NSAP prefixes requiring Integrated Services Digital Network numbers. These numbers include telephone numbers.

8.30.1.1 ICD

To create an ICD NSAP address, select **`Create`** from the NSAP Address dialog, then select ICD. The following fields are required to be filled:

Port Indicates the port number on which the NSAP prefix is to be created. The ports are numbered from the bottom left-hand side on the front of the switch.

VPI This is the number of the virtual path on which the NSAP prefix is to be created.

ICD Indicates the NSAP prefix for this entry.

DFI The Domain Specific Part Format Identifier.

AA The Administrative Authority. This identifier is assigned by ISO national member body.

RD Routing Domain identifier.

AREA Area identifies a unique area within a Routing Domain.

8.30.1.2 DCC

To create a DCC NSAP address, select **`Create`** from the NSAP Address dialog, then select DCC. The following fields are required to be filled:

Port Indicates the port number on which the NSAP prefix is to be created. The ports are numbered from the bottom left-hand side on the front of the switch.

VPI This is the number of the virtual path on which the NSAP prefix is to be created.

DCC Indicates the NSAP prefix for this entry.

DFI The Domain Specific Part Format Identifier.

AA The Administrative Authority. This identifier is assigned by ISO national member body.

RD Routing Domain identifier.

AREA Area identifies a unique area within a Routing Domain.

8.30.1.3 E.164

To create an E.164 NSAP address, select **`Create`** from the NSAP Address dialog, then select E.164. The following fields are required to be filled:

Port Indicates the port number on which the NSAP prefix is to be created. The ports are numbered from the bottom left-hand side on the front of the switch.

VPI This is the number of the virtual path on which the NSAP prefix is to be created.

E.164 Indicates the NSAP prefix for this entry.

RD Routing Domain identifier.

AREA Area identifies a unique area within a Routing Domain.

8.30.2 Static Routing

This menu option allows you to create, delete, and display NSAP static routes. You can reach this level by selecting a port or ports and then by pulling down the **`Configure/NSAP`** menu.

The following choices are available:

ICD This menu configures NSAP addresses requiring the International Code Designator (ICD). An ICD identifies an international organization.

DCC This menu configures NSAP addresses requiring the Data Country Code (DCC). A DCC specifies the country in which an address is registered.

E.164 This menu configures NSAP addresses requiring Integrated Services Digital Network numbers. These numbers include telephone numbers.

8.30.2.1 ICD

To create an ICD NSAP address, select **`Create`** from the NSAP Address dialog, then select ICD. The following fields are required to be filled:

ICD Indicates the complete 2-byte ICD NSAP address in hexadecimal format.

DFI The Domain Specific Part Format Identifier.

AA The Administrative Authority. This identifier is assigned by ISO national member body.

RD Routing Domain identifier.

AREA Area identifies a unique area within a Routing Domain.

ESI End System Identifier specifies an end system within an Area, and must be unique within an Area.

SEL The selector used by the end systems. Not used for ATM routing.

Mask This is the bit mask indicating number of high-order bits to use for routing purposes. The default mask for a static route to a host is 152. The default to a switch is 104.

Port Specifies the port through which this NSAP address can be reached.

VPI Specifies the UNI 3.x signalling path through which this NSAP address can be reached.

8.30.2.2 DCC

To create a DCC NSAP address, select **`Create`** from the NSAP Static Routing dialog, then select DCC. The following fields are required to be filled:

DCC Indicates the complete 2-byte DCC NSAP address in hexadecimal format.

DFI The Domain Specific Part Format Identifier.

AA The Administrative Authority. This identifier is assigned by ISO national member body.

RD Routing Domain identifier.

AREA Area identifies a unique area within a Routing Domain.

ESI End System Identifier specifies an end system within an Area, and must be unique within an Area.

SEL The selector used by the end systems. Not used for ATM routing.

Mask This is the bit mask indicating number of high-order bits to use for routing purposes. The default mask for a static route to a host is 152. The default to a switch is 104.

Port Specifies the port through which this NSAP address can be reached.

VPI Specifies the UNI 3.x signalling path through which this NSAP address can be reached.

8.30.2.3 E.164

To create an E.164 NSAP address, select **`Create`** from the NSAP Static Routing dialog, then select E.164. The following fields are required to be filled:

E.164 Indicates the complete 8-byte E.164 NSAP address in hexadecimal format.

RD Routing Domain identifier.

AREA Area identifies a unique area within a Routing Domain.

ESI End System Identifier specifies an end system within an Area, and must be unique within an Area.

SEL The selector used by the end systems. Not used for ATM routing.

Mask This is the bit mask indicating number of high-order bits to use for routing purposes. The default mask for a static route to a host is 152. The default to a switch is 104.

Port Specifies the port through which this NSAP address can be reached.

VPI Specifies the UNI 3.x signalling path through which this NSAP address can be reached.

8.30.3 Show ILMI

This menu option allows you to view NSAP addresses that are registered via ILMI. You can reach this option by selecting a port or ports and then by pulling down the **`Configure/NSAP`** menu.

The following information is available:

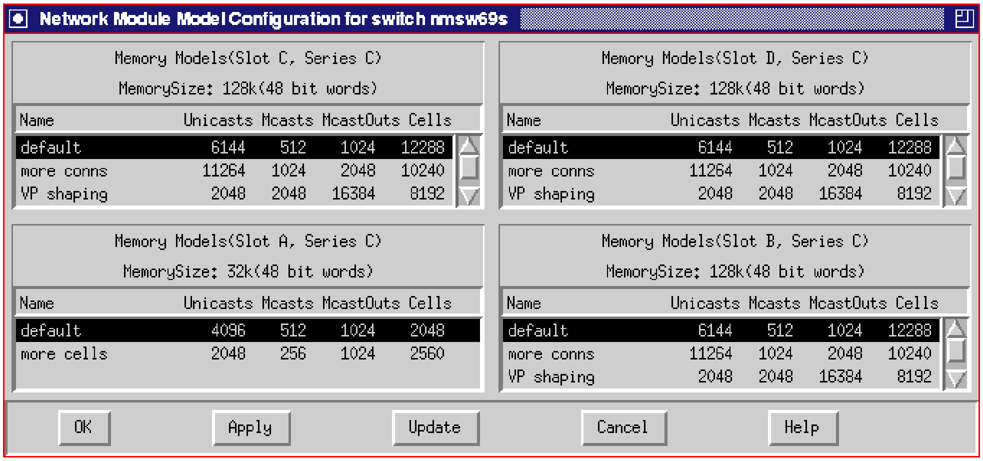
Port Identifies the port numbers registering NSAP addresses.

NsapAddress Identifies the NSPA address corresponding to the port number in the left column.

NOTE Click on the Update button to retrieve the most current NSAP information from the switch.

8.31 Models

This menu option allows you to select memory models for network modules that support shared memory (Series C and Series LC). You can reach this option by selecting a port or ports and then by pulling down the **`Configure/Models`** menu.



Network Module Model Configuration for switch nmsw69s

Memory Models(Slot C, Series C)
MemorySize: 128k(48 bit words)

Name	Unicasts	Mcasts	McastOuts	Cells
default	6144	512	1024	12288
more conns	11264	1024	2048	10240
VP shaping	2048	2048	16384	8192

Memory Models(Slot D, Series C)
MemorySize: 128k(48 bit words)

Name	Unicasts	Mcasts	McastOuts	Cells
default	6144	512	1024	12288
more conns	11264	1024	2048	10240
VP shaping	2048	2048	16384	8192

Memory Models(Slot A, Series C)
MemorySize: 32k(48 bit words)

Name	Unicasts	Mcasts	McastOuts	Cells
default	4096	512	1024	2048
more cells	2048	256	1024	2560

Memory Models(Slot B, Series C)
MemorySize: 128k(48 bit words)

Name	Unicasts	Mcasts	McastOuts	Cells
default	6144	512	1024	12288
more conns	11264	1024	2048	10240
VP shaping	2048	2048	16384	8192

Figure 8.33 - Shared Memory Network Module Dialog

Place the cursor on any of the five memory models and click on the **`Apply`** button to choose that model.

The fields in this display are defined as follows:

Name Displays the identifier for this shared memory configuration.

Unicasts For each model, shows the number of subnetwork-unicast connections supported.

Mcasts For each model, shows the number of non-unicast (i.e., subnetwork-broadcast or subnetwork-multicast) connections supported.

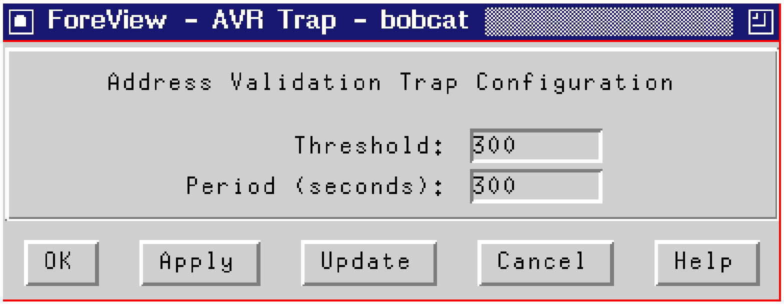
McastOuts For each model, shows the number of output multicast connections supported from the network module to the link for this shared memory model.

Cells For each model, shows the total amount of cell buffering that is supported for this shared memory model.

8.32 Address Validation

To perform address validation, select **AVR** from the **Configure** pull-down menu.

NOTE Address validation should be used only if your network includes one or more FORE switches that are being used as “edge” switches on the public side of a public network.



Address Validation Trap Configuration

Threshold: 300

Period (seconds): 300

Figure 8.34 - Address Validation Dialog

The fields in this display are defined as follows:

Threshold Displays the Public-AV Address Threshold. Default is 300 rejected cells.

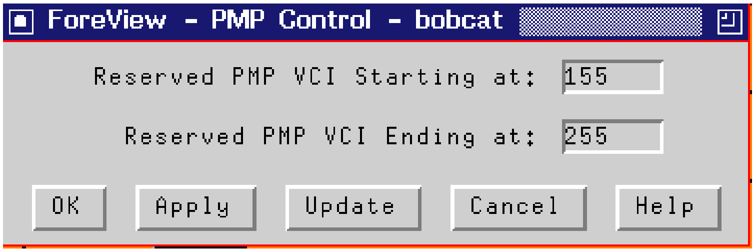
Period (seconds) Displays the Public-AV Address Timespan. Default is 300 seconds.

8.33 PMP Configuration

To set the minimum and maximum number for the range of VCIs that are reserved for point-to-multipoint connections, select **PMP** from the **Configure** pull-down menu. This allows a block of VCIs to be reserved for LAN Emulation point-to-multipoint use. This block of VCIs is reserved on all paths and on all ports on this switch fabric. PVCs can be created on these VCIs, but no point-to-point connections may use these VCIs.

NOTE

PMP configuration is useful only when the switch is running in non-extended mode. For more information about non-extended mode, please see the *ForeRunner* ATM Switch User's Manual.


ForeView - PMP Control - bobcat

Reserved PMP VCI Starting at: 155

Reserved PMP VCI Ending at: 255

Figure 8.35 - Point-to-Multipoint Reserved VCI Control Dialog

The fields in this display are defined as follows:

Reserved PMP VCI Starting at: Indicates the bottom number for the range of VCIs to be reserved for point-to-multipoint connections. The default is 155.

Reserved PMP VCI Ending at: Indicates the top number for the range of VCIs to be reserved for point-to-multipoint connections. The default is 255.

8.34 PNNI-SPVC Pace and Reroute Configuration

To set pacing and rerouting parameters, select **PNNI-SPVC** from the **Configure** pull-down menu.

8.34.1 Pacing

Pacing parameters regulate the call setup cycle for SPVCs that are "down" (established, but currently not active). If a switch has a large number of SPVCs configured in the CDB, it tries to open the SPVCs all at once when it reboots. Therefore, it is advantageous to pace the number of SPVCs that are opened at once, so that each is serviced properly.

This pacing allows you to set the SPVC controller to open only the configured number of SPVCs and to schedule itself for callback after the specified time interval if there are more SPVCs to be opened, both at start up and at the retry callback.

The pacing cycle is as follows:

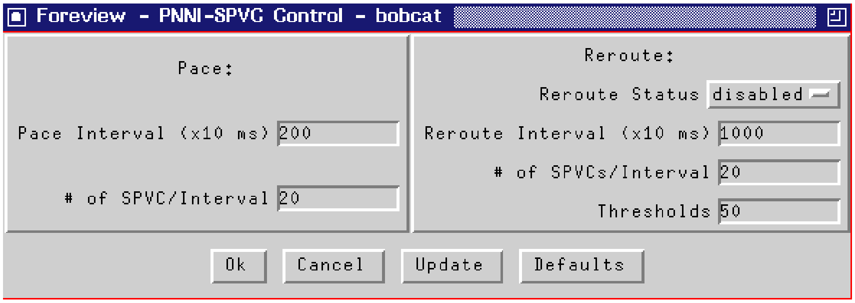
1. Attempt an established number of SPVC call setups for down SPVCs.
2. Pause for an established interval (in seconds).
3. Return to step 1.

8.34.2 Rerouting

Rerouting parameters regulate whether or not to evaluate the efficiency of the routes used by the "up" (established and currently active) PNNI SPVCs. If enabled, the rerouting cycle is as follows:

1. Check the current call routing cost for the number of up PNNI SPVCs. (The call routing cost is the sum of all the link costs over the call route.)
2. Check to see if better (new call routing cost is less by the threshold percentage) routes are available. If so, disconnect and reroute (attempting to reconnect using the pacing cycle) those that can be improved and go to step 3. If not, go to step 3.
3. Pause for an established interval (in seconds).
4. Return to step 1.

Sometimes SPVCs are forced to use a non-optimal route because of temporary link failures or because of an inconsistent routing database. Rerouting lets you configure the SPVC controller to check for SPVCs that are using sub-optimal routes and reroute them if a better route becomes available. A path is considered "better" than another path if its administrative weight is lower by a specified percentage.



Pace:

Pace Interval (x10 ms) 200

# of SPVC/Interval 20

Reroute:

Reroute Status disabled

Reroute Interval (x10 ms) 1000

# of SPVCs/Interval 20

Thresholds 50

Figure 8.36 - PNNI-SPVC Control Dialog

The fields in this display are defined as follows:

Pace Interval (x10 ms) Indicates the interval in seconds between call setup attempts. Values can be from **1** to **300** seconds. The default is **2** seconds.

# of SPVC/Interval Indicates the number of call setups to attempt. Values can be from **1** to **1000**. The default is **20** calls.

Reroute Status Allows you to enable or disable the PNNI SPVC rerouting feature. Enable indicates that you want to begin checking for and rerouting SPVCs that are using sub-optimal routes. Disable indicates that you want to stop checking for and rerouting SPVCs that are using sub-optimal routes. This is the default state for PNNI SPVCs.

Reroute Interval (x 10 ms) Indicates the time interval, in milliseconds, between successive callbacks to the SPVC controller to check for and reroute existing SPVC connections if a better path becomes available. The default is **1000** milliseconds (10 seconds). The range of valid values is **100** to **360000**, inclusive.

# of SPVCs/Interval Indicates how many up SPVCs, per interval, will be analyzed to determine whether or not those SPVCs need to be rerouted. The default is **20** SPVCs. The range of valid values is **1** to **1000**, inclusive.

Thresholds Indicates the minimum percentage improvement in the cost that the new SPVC path must have over the current SPVC path before a reroute is performed. The default value is **`50`** percent. The range of valid values is **`1`** to **`99`**, inclusive.

8.35 SCP Configuration

This section explains how to configure failover support in the ASX-200BX and ASX-1000 when two SCPs are installed in a single switch fabric.

NOTE

Only HA-based processors provide dual SCP support. An HA-based processor is labelled SCP-ASXHA on the lower left corner of its faceplate.

When two SCPs are installed in a switch fabric, the switch recognizes their presence and automatically runs in dual SCP mode. When the switch boots, the SCP which resides below network module slots A and C (slot X) is designated as the primary SCP by default. The SCP which resides in the slot below network module slots B and D (slot Y) is designated as the standby SCP by default. The front panel of an ASX-200BX or ASX-1000 switch graphically represents the dual SCPs by labelling the control ports as **`active`** and **`standby`**, as shown in the following figure.

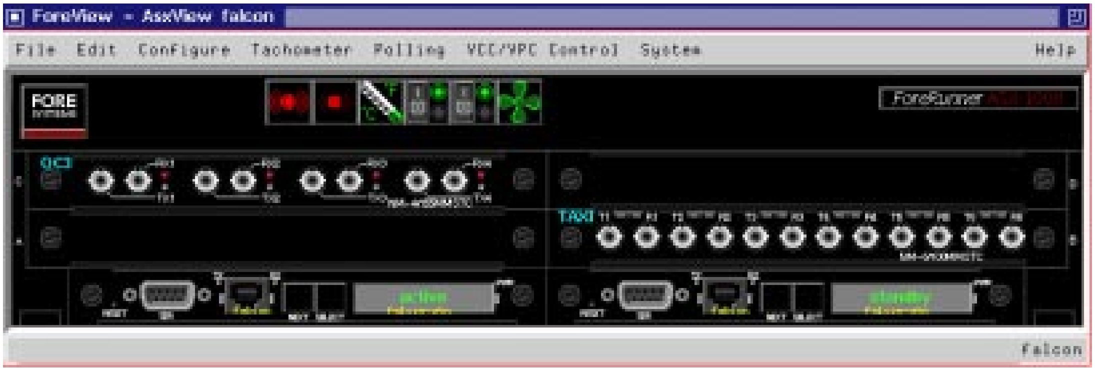


Figure 8.37 - ASX-1000 Front Panel with Dual SCPs

While in dual SCP mode, the controlling SCP emits a “heartbeat” at regular intervals. This heartbeat is monitored by the standby SCP. In the event of a hardware failure on the controlling SCP, the heartbeat disappears and the standby SCP takes over.

Switch configuration information (i.e., CDB configuration, FLASH configuration, etc.) can be synchronized between the controlling and standby SCP so that this information is maintained if SCP failover occurs.

If a failure is detected on the controlling SCP, the standby SCP will initiate a cold restart of the switch. After the switch restarts, PVCs are re-established, and switch configuration information is restored, depending the level of synchronization that was configured between the two SCPs.

NOTE SVCs will have to be restored manually after a restart.

NOTE Dual SCPs in a switch fabric DO NOT provide redundancy, only failover support. The two SCPs do not share the task of controlling the switch fabric, they simply exist as an immediate backup in the event of a failure.

8.35.1 Dual SCP Configuration Menu

The front panel provides configuration dialogs that allow you to configure failover support, including the designation of the primary and secondary SCPs, in ASX-200BX and ASX-1000 switches when two SCPs are installed in a single switch fabric. To access the menus for SCP configuration, select one of the control ports (**`primary`** or **`standby`**), right click over port, and select **`Dual SCP`**. The configuration menu options are defined as follows:

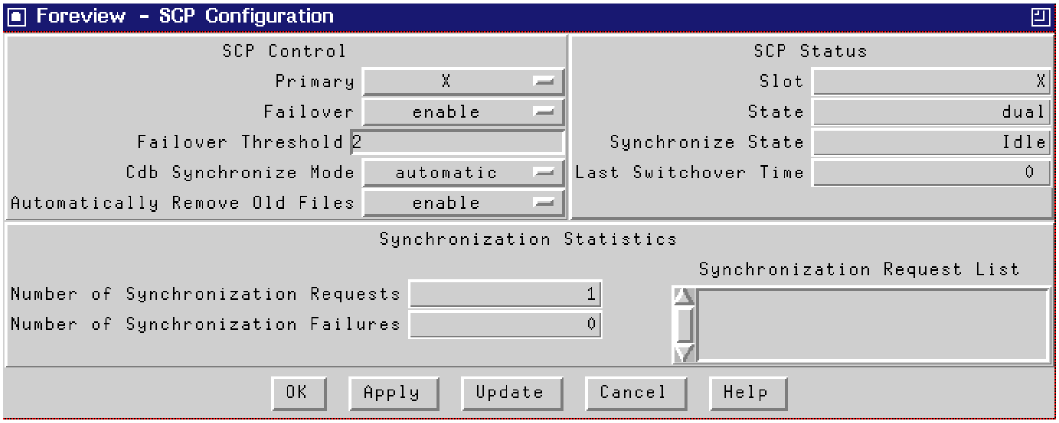
Dual SCP / Configuration Select this option to designate the primary and standby SCP, check the status of the SCP, and view synchronization statistics.

Dual SCP / Synchronize Select this option to synchronize the information contained on both SCPs to ensure a reliable failover mechanism.

Dual SCP / Switchover Select this option to force the standby SCP to take control of the switch.

Dual SCP / Reboot Standby Select this option to force the standby SCP to reboot.

Select a control port and right click the mouse button to select **`Dual SCP/Configuration`** to launch the **`SCP Configuration`** dialog, shown in the following figure. From this dialog, you can designate the primary and standby SCP, check the status of the SCP, and view synchronization statistics.


Foreview - SCP Configuration
SCP Control
SCP Status
Synchronization Statistics
Synchronization Request List
OK
Apply
Update
Cancel
Help

Primary X
Failover enable
Failover Threshold 2
Cdb Synchronize Mode automatic
Automatically Remove Old Files enable

Slot X
State dual
Synchronize State Idle
Last Switchover Time 0

Number of Synchronization Requests 1
Number of Synchronization Failures 0

Figure 8.38 - SCP Configuration Dialog

The fields of this dialog are defined as follows:

8.35.1.1 SCP Control

Primary This toggled option lets you designate which SCP is to control the switch at start-up. To designate the primary SCP, select X. This indicates that the SCP in the left slot of the switch fabric (the top slot in an ASX-1000) is the primary SCP. This is the default.

Select Y to designate that the SCP in the right slot of the switch fabric (the bottom slot in an ASX-1000) is the primary SCP.

NOTE

The primary SCP and the controlling are not necessarily the same. “Primary” refers to the SCP that is supposed to control the switch after it boots. “Controlling” refers to the SCP that actually controls the switch. For example, if the SCP in slot X fails at start-up, the SCP in slot Y will control the switch even though it is not designated as the primary SCP.

Failover This toggled option lets you enable or disable failover to a second SCP in the event of a hardware failure on the controlling SCP. Enable indicates that SCP failover will be enabled. This is the default. Disable indicates that SCP failover will be disabled.

CAUTION

If failover is disabled, the standby SCP will not take control of the switch fabric if the controlling SCP fails, regardless of how other SCP parameters are set.

Failover Threshold This option lets you set the threshold time, in seconds, that the standby SCP will wait to receive a heartbeat from the controlling SCP before taking control of the switch. The minimum and default value is 2 seconds.

Cdb Synchronize Mode This toggled option lets you set the synchronization mode for the Cdb (Configuration database). Select **`automatic`** to set Cdb synchronization between the primary and standby SCPs automatically. Select **`manual`** to disable automatic Cdb synchronization. The default is **`automatic`**.

Automatically Remove Old Files This toggled option allows unused files and directories to be removed from the FLASH of the standby SCP. To ensure a reliable failover mechanism, the information contained on both SCPs should be synchronized. If free space on the FLASH of the standby SCP is depleted during a synchronization attempt, the standby SCP removes unused files and directories if **`enable`** is selected.

If **`disable`** is selected, synchronization attempts fail in the event that there is not enough free space in FLASH. This is the default.

8.35.1.2 SCP Status

Slot Shows which SCP (X or Y) is the primary SCP. The SCP in slot **`X`** is set to **`primary`** by default.

State Shows the state of the SCP. **`standalone`** indicates that there is only one SCP in the switch fabric. **`dual`** indicates that there are two SCPs installed in the switch fabric, and the SCPs are communicating with one another. **`other`** indicates that there are two SCPs installed in the switch fabric, but they are not communicating with one another.

Synchronize State Shows the state of the current synchronization attempt between the controlling and standby SCP. **`Suspended`** means either that the switch is not in dual SCP mode, or that the SCPs are running different versions of switch software. **`Idle`** means that synchronization is not taking place between SCPs. **`Manual`** means that a manual synchronization is taking place between SCPs. **`Automatic`** means an automatic synchronization is taking place between SCPs.

NOTE When manual or automatic synchronization is taking place between SCPs, the name of the file being synchronized is also displayed.

Last Switchover Time Indicates the date and timestamp that the standby SCP was forced to take control of the switch.

8.35.1.3 Synchronization Statistics

Number of Synchronization Requests Shows the number of synchronization requests that have been made between the controlling and standby SCP.

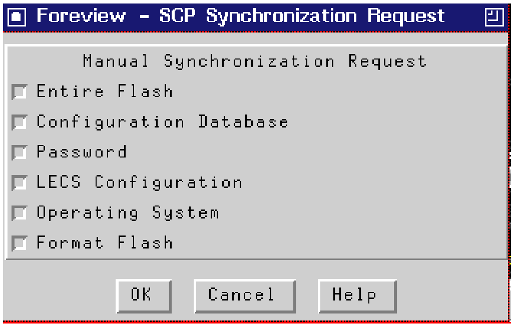
Number of Synchronization Failures Shows the number of synchronizations requests that have failed between SCPs.

Synchronization Request List Shows how many synchronization requests are waiting to be processed.

8.35.2 SCP Synchronization Request

To ensure a reliable failover mechanism, the information contained on both SCPs should be synchronized. This can be done automatically through the **`Dual SCP/Configuration`** menu described in the previous section. Synchronization also can be requested manually via the **`Dual SCP/Synchronize`** menu.

Select a control port and right click the mouse button to select **`Dual SCP/Synchronize`** to launch the **`SCP Synchronization Request`** dialog, shown in the following figure. From this dialog, you can initiate synchronization requests for the FLASH, CDB, password file, LECS configuration, and switch software version.



Foreview - SCP Synchronization Request

Manual Synchronization Request

□ Entire Flash

□ Configuration Database

□ Password

□ LECS Configuration

□ Operating System

□ Format Flash

Figure 8.39 - Manual SCP Synchronization Request Dialog

The fields of this dialog are defined as follows:

Entire Flash Indicates that all directories and files in FLASH on the controlling SCP will be copied to the standby SCP.

Configuration Database Indicates that the Configuration Database (CDB) will be copied from the controlling to the standby SCP.

Password Indicates that the password file will be copied from the controlling SCP to the standby SCP.

LECS Configuration Indicates that the LAN Emulation Configuration Services (LECS) configuration file will be copied from the controlling to the standby SCP.

Operating System Indicates that the switch software will be copied from the controlling SCP to the standby SCP.

NOTE Only the current version of switch software is copied to the standby SCP.

Format Flash Indicates that the FLASH on the standby SCP will be re-initialized.

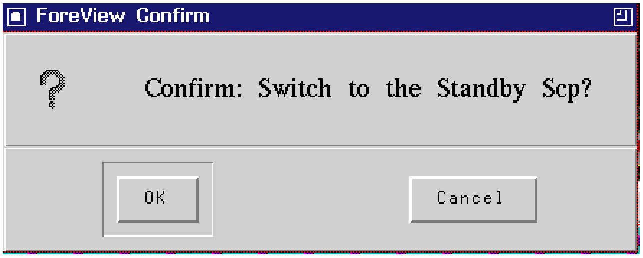
CAUTION

Using the **Format Flash** option formats the FLASH on the standby SCP. This removes all information on the FLASH.

8.35.3 Switching over to the Standby SCP

If you wish to force the standby SCP to take control of the switch, select a control port and right click the mouse button to select **Dual SCP/Switchover.** This option provides the ability to force a switchover from the controlling to the standby SCP.

You will be asked to confirm this selection. Select **OK** at the confirm dialog to reset the standby SCP. Select **Cancel** at the dialog to cancel the selection.

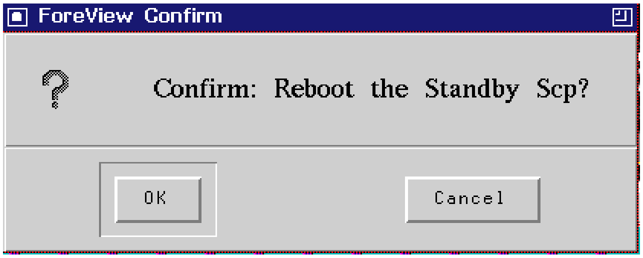


Confirm: Switch to the Standby Scp?

Figure 8.40 - Confirm Switchover Dialog

8.35.4 Resetting the Standby SCP

If you wish to force the standby SCP to reboot, select a control port and right click the mouse button to select **Dual SCP/Reboot Standby.** You will be asked to confirm this selection. Select **OK** at the confirm dialog to reboot the standby SCP. Select **Cancel** at the dialog to cancel the selection.



ForeView Confirm

Confirm: Reboot the Standby Scp?

Figure 8.41 - Confirm Reboot Standby SCP Dialog

CHAPTER 9 Connection Management

ATM is a switched, connection-oriented technology in which information, in the form of cells, is transferred through the network via switched virtual connections. The components that make up virtual connections are the media, virtual paths (VPs), and virtual channels (VCs). Essential to ATM virtual connections is the quality of service (QoS) related to the bandwidth parameters associated with the virtual connections.

ForeView provides a tool for the provisioning and management of virtual connections. The Virtual Path / Channel Tool is found under the "VCC / VPC Control" menu in the *ForeView* Front Panel, first mentioned in Chapter 8 and covered in greater detail in this chapter.

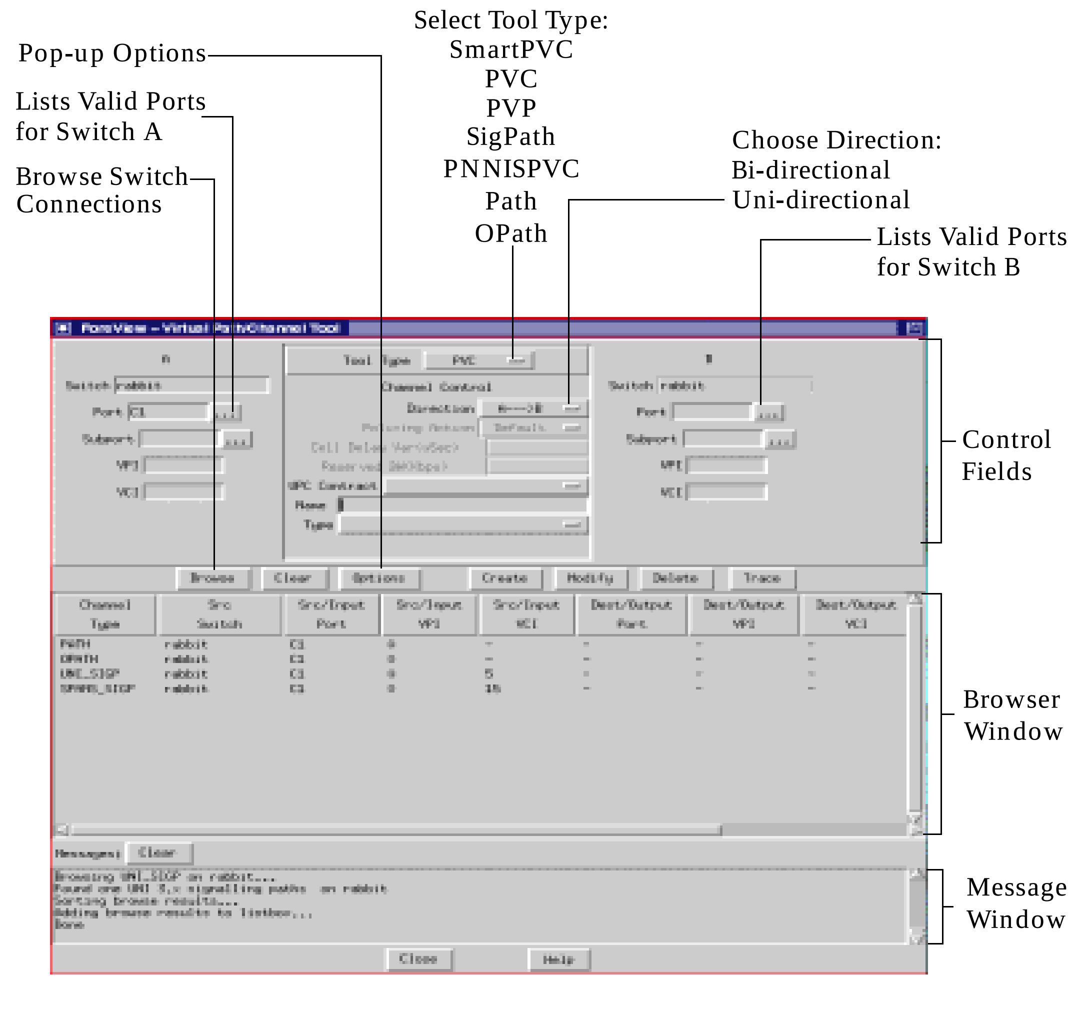
The Virtual Path / Channel Tool provides seven options that allow for the browsing, creation, and deletion of virtual paths, virtual circuits, and signalling paths on a FORE ATM switch. Those seven options are:

- PVCs (Permanent Virtual Circuits), which are virtual circuits between endpoints in a network. A circuit is made up of a series of interconnected permanent channels provisioned on each switch along the circuit path. PVCs often are necessary in order to inter-operate with multi-vendor equipment. PVCs also can be used to provide connections with guaranteed bandwidth or QoS.
- Smart PVCs, which are virtual circuits between endpoints in a network. The circuit is made up of a series of signalled channels provisioned from the endpoints. If a link carrying a SPVC goes down and there is an alternate route, then the end switch fabrics of the SPVC automatically reroute the SPVC around the failed link.
- PVPs (Permanent Virtual Paths), which are through paths identified by a Virtual Path Identifier (VPI) and a QoS.
- Signalling Paths, which are either UNI 3.x signalling paths or SPANS (FORE's proprietary signalling protocol) signalling paths. Signalling paths allow the use of SVCs (Switched Virtual Circuits), which are dynamically established connections.

- PNNISPVCs, which are *ForeThought* PNNI SPVCs. These connections are inherently bidirectional, which means that a single signalling call establishes the circuits in both directions.
- Paths (Incoming Paths), which are required for creating PVCs. If you attempt to create a PVC with no corresponding incoming path, the Virtual Path/Channel Tool prompts you to create the path.
- OPaths (Outgoing Paths), which also are required for creating PVCs. Again, when you attempt to create a PVC with no corresponding outgoing path, the Virtual Path/Channel Tool prompts you to create the paths.

9.1 The Virtual Path/Channel Tool

The following sections define the Virtual Path/Channel Tool options found under the VCCs menu bar. This tool, shown in Figure 9.1, has all the options necessary to create VCs through an ATM network.



A

Switch rabbit

Port C1

Subport

VPI

VCI

Tool Type PVC

Channel Control

Direction A--->B

Policing Action Default

Cell Delay Var(uSec)

Reserved BW(Kbps)

UPC Contract

Name

Type

B

Switch rabbit

Port

Subport

VPI

VCI

Channel Type	Src Switch	Src/Input Port	Src/Input VPI	Src/Input VCI	Dest/Output Port	Dest/Output VPI	Dest/Output VCI
PATH	rabbit	C1	0	-	-	-	-
OPATH	rabbit	C1	0	-	-	-	-
UNI_SIGP	rabbit	C1	0	5	-	-	-
SPANS_SIGP	rabbit	C1	0	15	-	-	-

Messages:

```
Browsing UNI_SIGP on rabbit...
Found one UNI 3.x signalling paths  on rabbit
Sorting browse results...
Adding browse results to listbox...
Done
```

Figure 9.1 - Virtual Path/Channel Tool

The Virtual Path/Channel Tool allows the browsing, creation, and deletion of permanent virtual channels. Please refer to the Appendix "An Overview of Virtual Connections" for additional explanation of the purpose and semantics of channels. The following sections explain the various fields and their values.

9.1.1 Tool Type

Pull down this menu to select what type of circuit or signalling path to create. The seven options are:

SmartPVC Select this item to create Smart PVCs.

PVC Select this item to create PVCs.

PVP Select this item to create through paths.

SigPath Select this item to create UNI 3.x or SPANS signalling paths.

PNNI SPVC Select this item to create *ForeThought* PNNI Smart PVCs.

Path Select this item to create incoming paths.

OPath Select this item to create outgoing paths.

9.1.2 Channel Control

The upper portion of the Virtual Path/Channel Tool contains the control fields that allow you to select the endpoints for channel creation, modification, deletion, or browsing. The fields under the labels A and B are used for channel creation, modification, deletion, or browsing. When using the Virtual Path/Channel Tool, remember the following points:

- For browsing, entries are not required for every field. For example, you may browse for circuits with only the switch name entered.
- For PVCs, switch B must be the same as switch A, and the fields under switch B will be read-only.
- The fields under Channel Control in the center of the dialog are used for creation, modification, and deletion of paths and channels only.

NOTE Control fields are filled in automatically when an existing path or circuit is chosen using the browser.

NOTE

When creating signalling paths, additional parameters required for SPANS or UNI 3.x signalling paths will replace the switch B control fields.

9.1.3 Command Buttons

The Virtual Path / Channel Tool provides several command buttons to manipulate virtual connections. The following section explains the various command buttons and their functions.

Browse The **Browse** button is used to scan virtual channels and paths on a switch. The results of the browse are dictated by what types of links are selected under the **Path & Channel Types** list in the **Options** dialog.

Clear The **Clear** button clears all entries from the input fields. In *ForeThought* software version 3.3 or earlier the **Clear** button also fills in the Policing Action and CDV values from the switch-wide values.

Options The **Options** button allows finer control of the scope of the browse function, which can be modified by via the **Options** dialog box. Browsing can be limited by filling in one or more of the port, VPI, or VCI entries. If a channel is selected in the browser by clicking on it with the left mouse button, the selected channel will be loaded into the Channel Tool fields for further operations.

Create The **Create** button allows a channel of the chosen values to be created on the switch. If you attempt to create a PVC with no corresponding incoming or outgoing path, the Tool prompts you to create the paths. Once the required paths have been created, the **Create** button can be selected again to create the channel.

Modify The **`Modify`** button allows connection parameters to be changed without bringing the connection down.

Delete The **`Delete`** button causes a channel of the chosen values to be destroyed on the switch.

Trace The **`Trace`** button traces the selected VC and displays the output in the messages window.

Close The **`Close`** button dismisses the Virtual Path/ Channel Tool.

9.1.3.1 Command Button Modes

The functionality of the **`Create/Modify/Trace/Delete`** command buttons depends on the mode of the Virtual Path/Channel Tool. There exists a three-state modality that defines the availability of a command button:

1. Unknown, indicating that a condition exists where some or all of the key fields of the tool type are missing;
2. Exist, indicating that a condition where all of the key fields of the tool type are present and the link described by the key fields exists on the switch;
3. Absent, indicating that a condition where all of the key fields of the tool type are present but the link described by the key fields does not exist on the switch.

A transition between mode states can occur during the following events:

- A key field has been modified
- The tool type has been changed
- The link direction has been changed
- A link has been selected from the Browse list
- The signalling type (SPANS vs. UNI 3.x) has been changed

The distinction between the Exist and Absent state is made by querying the switch each time a change state event occurs. The **`Modify`** function is available during the Exist state depending on whether the link is modifiable.

The following table summarizes the command functions with respect to the mode state.

Table 9.1 - Command Mode Summary

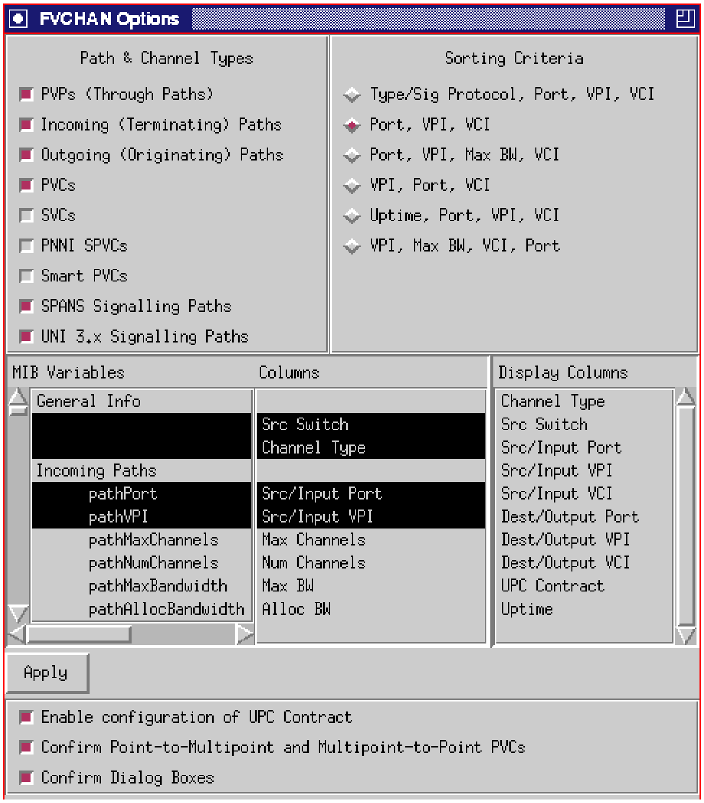
Function	States		
	Unknown	**Exist**	**Absent**
Create Button	Inactive	Inactive	**Active**
Modify Button	Inactive	**Active**	Inactive
Delete Button	Inactive	**Active**	Inactive
Trace Button	Inactive	**Active**	Inactive

Before proceeding with a command, the following validation steps occur:

- The **`Create`** function validates to ensure that the link being created does not exist. If it does exist, the user is queried whether to proceed with a **`Modify`** action instead.
- The **`Modify`** function validates to ensure that the link being modified does exist. If it does not exist, the user is queried whether to proceed with a **`Create`** action instead.
- The **`Delete`** function validates to ensure that the link exists. If it does not exist, an error message is presented.

9.2 Tool Options

Select the **`Options`** button on the Virtual Path / Channel Tool front panel for more specific control of the scope of the browse function. This dialog provides user-configurable filter, display column, and sorting options. Figure 9.2 shows the Virtual Path / Channel Tool Options dialog.



Path & Channel Types

- ☒ PVPs (Through Paths)
- ☒ Incoming (Terminating) Paths
- ☒ Outgoing (Originating) Paths
- ☒ PVCs
- □ SVCs
- □ PNNI SPVCs
- □ Smart PVCs
- ☒ SPANS Signalling Paths
- ☒ UNI 3.x Signalling Paths

Sorting Criteria

- ○ Type/Sig Protocol, Port, VPI, VCI
- ● Port, VPI, VCI
- ○ Port, VPI, Max BW, VCI
- ○ VPI, Port, VCI
- ○ Uptime, Port, VPI, VCI
- ○ VPI, Max BW, VCI, Port

MIB Variables	Columns
General Info	
	Src Switch
	Channel Type
Incoming Paths	
pathPort	Src/Input Port
pathVPI	Src/Input VPI
pathMaxChannels	Max Channels
pathNumChannels	Num Channels
pathMaxBandwidth	Max BW
pathAllocBandwidth	Alloc BW

Display Columns

Channel Type
Src Switch
Src/Input Port
Src/Input VPI
Src/Input VCI
Dest/Output Port
Dest/Output VPI
Dest/Output VCI
UPC Contract
Uptime

- ☒ Enable configuration of UPC Contract
- ☒ Confirm Point-to-Multipoint and Multipoint-to-Point PVCs
- ☒ Confirm Dialog Boxes

Figure 9.2 - Virtual Path / Channel Tool Options

9.2.1 Filtering by Path and Channel Type

The Virtual Path/Channel Tool provides filters that allow you to browse specific path and channel types. For a selected switch, browsing can be turned on or off for the following:

- PVPs (Permanent Virtual Paths) or Permanent Through Paths are paths used for dedicated long-term aggregate channel transport between locations.
- PVCs (Permanent Virtual Circuits (or Channels)), which are circuits or channels used for dedicated long-term information transport between locations.
- SVCs (Switched Virtual Circuits (or Channels)).
- Smart PVCs, simplified PVCs in which circuits or channels used for dedicated long-term information transport between locations, they are permanently provisioned at each endpoint, and are switched between endpoints. Smart PVCs use the SPANS signalling protocol for SVC setup.
- Outgoing (Originating) Paths, types of PVPs (Permanent Virtual Paths), which are points at which a virtual path originates.
- Incoming (Terminating) Paths, types of PVPs (Permanent Virtual Paths), which are points at which a virtual path terminates.
- SPANS signalling paths, which use FORE’s proprietary signalling protocol for establishing SVCs between FORE equipment.
- UNI 3.x signalling paths, which use the ATM Forum standard signalling protocol.
- PNNI SPVCs, which are *ForeThought* PNNI SPVCs used for dedicated long-term information transport between locations. They are provisioned at each endpoint, and are switched between endpoints. PNNI SPVCs use UNI 3.x signalling protocol for SVC setup.

Selecting any of the path and channel types does not affect the current state of the browse display. To use the path and channel types for filtering, do the following:

1. Select one or more of the path and channel types (a red button indicates the item is selected).
2. Close the Options menu.
3. At the Virtual Path/Channel Tool, click on the **`Browse`** button to update the display.

The output will reflect the selected filter options.

9.2.2 Enabling Configuration of UPC Contracts

The Virtual Path / Channel Tool provides an option that, when enabled, allows the configuration and selection of UPC contracts. When disabled, you only can select UPC contracts via the Virtual Path / Channel Tool. The **`Options`** dialog allows you to enable or disable this feature. This resource is part of the *ForeView* configuration file as well.

9.2.3 Showing P-MP and MP-P Confirmation Dialog Boxes

The Virtual Path / Channel Tool provides confirmation boxes when you are creating a PVC that is either a point-to-multipoint (p-p) or a multipoint-to-point (mp-p) connection. The **`Options`** dialog allows you to turn these confirmation dialog boxes on or off. This resource is part of the *ForeView* configuration file as well.

9.2.4 Showing Confirmation Dialog Boxes

The Virtual Path / Channel Tool provides confirmation boxes for many of the actions related to the creation / deletion of VCCs. The **`Options`** dialog allows you to turn these confirmation dialog boxes on or off. This resource is part of the *ForeView* configuration file as well.

9.2.5 Sorting Criteria

The Virtual Path / Channel Tool allows you to sort the permanent virtual circuits on a selected switch based on the following criteria:

- Type / Sig Protocol, Port, VPI, VCI
- Port, VPI, VCI
- Port, VPI, Max BW, VCI
- VPI, Port, VCI
- Uptime, Port, VPI, VCI
- VPI, Max BW, VCI, Port

When sorting, remember the following points:

- A red button indicates which sorting criteria is selected.
- Sorting is alphanumeric in increasing order.
- Only one sorting criteria may be selected at any time.
- Changing from one sorting criteria to another is automatically reflected on the main display of the Virtual Path / Channel Tool.

9.2.6 Display Columns

The Virtual Path / Channel Tool allows you to select which connection variables are displayed on the front panel of the tool. The fields available for display on the Tool dialog are selected from the Columns list in the center of the Options dialog. The display choices are organized by path and channel types, and the related MIB variable for each type is provided in the MIB Variables column. The order of the Virtual Path / Channel Tool front panel can be re-arranged by moving the display columns.

9.2.6.1 Moving Columns

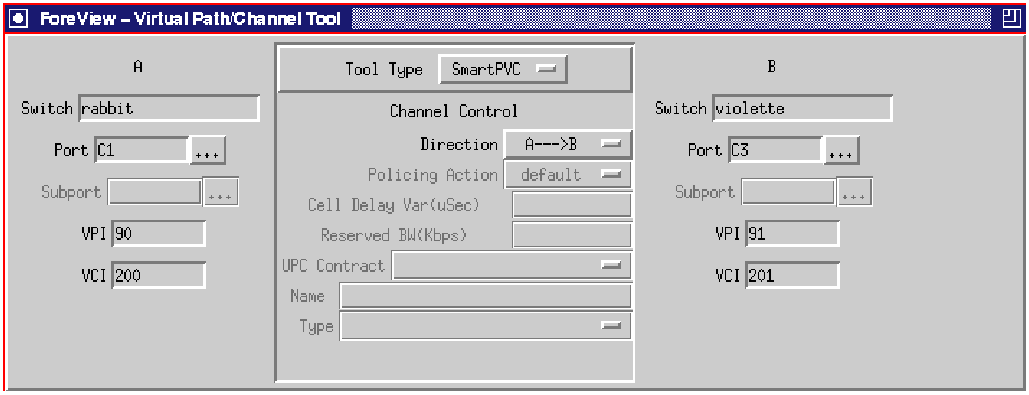
The order of the Virtual Path / Channel Tool front panel can be re-arranged by moving columns. When moving columns, remember the following points:

- Select the column you want to move by clicking on the header of the column.
- Position the cursor on the column header where you want to place the selected column and click the mouse button. This action inserts the selected column in this new position, and the other columns are displaced one position to the right.

9.3 Creating Smart PVCs

Select tool type SmartPVC to browse, create and delete SPVCs (Smart Permanent Virtual Circuits). An SPVC is a connection that goes across multiple switch fabrics. An SPVC looks like a PVC at the local and remote endpoints with an SVC in the middle. SPVCs are more robust than PVCs. If a link carrying a PVC goes down, then the PVC goes down. If a link carrying an SPVC goes down and there is an alternate route, then the end switch fabrics of the SPVC automatically reroute the SPVC around the failed link. Figure 9.3 shows the Smart PVC tool dialog.

NOTE For Smart PVCs to work, SPANS signalling must be enabled for the path being used.


ForeView – Virtual Path/Channel Tool

A
Switch rabbit
Port C1
Subport
VPI 90
VCI 200

Tool Type SmartPVC
Channel Control
Direction A--->B
Policing Action default
Cell Delay Var(uSec)
Reserved BW(Kbps)
UPC Contract
Name
Type

B
Switch violette
Port C3
Subport
VPI 91
VCI 201

Figure 9.3 - Smart PVC Tool Dialog

9.3.1 Key Fields for the Smart PVC Tool

To create an SPVC, you must configure the two ends concurrently on the two switch fabrics. Therefore, you must have a valid session open on both the local switch fabric (Switch A) and the destination switch fabric (Switch B). These fields are filled in automatically when an existing SPVC is chosen using the browser. The key fields for control of the Smart PVC tool are defined as follows:

Switch A and B

Port The number of the port where the circuit enters the switch.

Subport Launches the sub-port timeslot configuration dialog. This configuration option is available only when selecting ports from FORE Systems' Circuit Emulation Services (CES) DS1 and E1 network modules.

VPI The Virtual Path Identifier (VPI) on which the circuit enters the switch.

VCI The Virtual Channel Identifier (VCI) on which the circuit enters the switch.

9.3.2 Optional Fields for the Smart PVC Tool

The optional control fields for the Smart PVC tool are defined as follows:

Direction Toggled selection for path creation. Choices are bi-directional (<-->), and uni-directional (--> or <--). The default value is bi-directional.

Reserved BW (Kbps) The amount of peak reserved bandwidth for the circuit or path in kilobits per second.

NOTE

Policing Action and Cell Delay variation are disabled in the Smart PVC tool.

9.3.3 CES Configuration for Smart PVCs

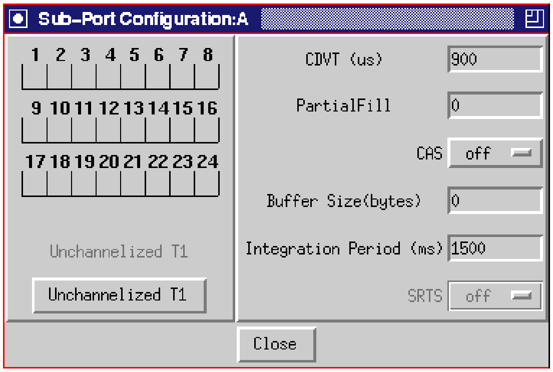
The CES-DS1 and CES-E1 network modules provide adaptation from time-division multiplexed (TDM) equipment (i.e., PBXs, WAN multiplexers, channel banks, video codecs, etc.) and traffic to ATM. Both modules provide structured and unstructured services, with a maximum of 127 connections supported on each module.

- For DS1 CES network modules all six ports may support fractional DS1 services (n x 56 Kbps/n x 64 Kbps) where 1 to 24 contiguous or non-contiguous DS0 channels are mapped to a single ATM VCC not to exceed 127 total connections.
- For E1 CES network modules all six ports may support fractional E1 services (n x 56 Kbps/n x 64 Kbps) where 1 to 31 contiguous or non-contiguous DS0 channels are mapped to a single ATM VCC not to exceed 127 total connections.

Structured services provide digital access and cross-connect system (DACS) like functions where n x 64 Kbps and n x 56 Kbps digital signal level zero (DS0) channels are adapted to ATM cells and mapped to unique ATM virtual connections (VCCs).

Unstructured services provide support and maintenance of a single full bandwidth 1.544 Mbps (DS1) or 2.048 Mbps (E1) clear channel across a single ATM virtual connection.

When you select a port from either of the CES-DS1 and CES-E1 network modules when configuring a Smart PVC, and then select **`Subport`**, the dialog in Figure 9.4 is displayed.



Sub-Port Configuration:A

CDVT (us) 900

PartialFill 0

CAS off

Buffer Size(bytes) 0

Integration Period (ms) 1500

SRTS off

Unchannelized T1

Figure 9.4 - CES Subport Configuration Dialog (DS1)

The key control fields for the subport configuration are defined as follows:

CDVT (us) Indicates the Cell Delay Variation Tolerance for cells being received by the segmentation and reassembly (SAR) engine.

PartialFill Indicates the amount of partialfill used, (i.e. how much of the ATM cell contains data and how much is filler). The default value is 47 bytes, for 47 bytes of data. The allowable range for DS1 CES is 9 - 47 bytes.

CAS Indicates whether Channel Associated Signalling (CAS) is to be used on the connection. The default is `no`.

Buffer Size (bytes) Indicates the amount of reassembly buffer space allocated for the connection. The default is 512 bytes per timeslot.

Integration Period (ms) Indicates the amount of time allocated to re-establish the connection before, while, or after the call is established, or in the case of interruption.

SRTS Indicates whether Synchronous Residual Time Stamp (SRTS) clock recovery is to be enabled on this connection. `on` indicates that SRTS is enabled, `off` indicates that SRTS is disabled. SRTS is disabled by default.

NOTE

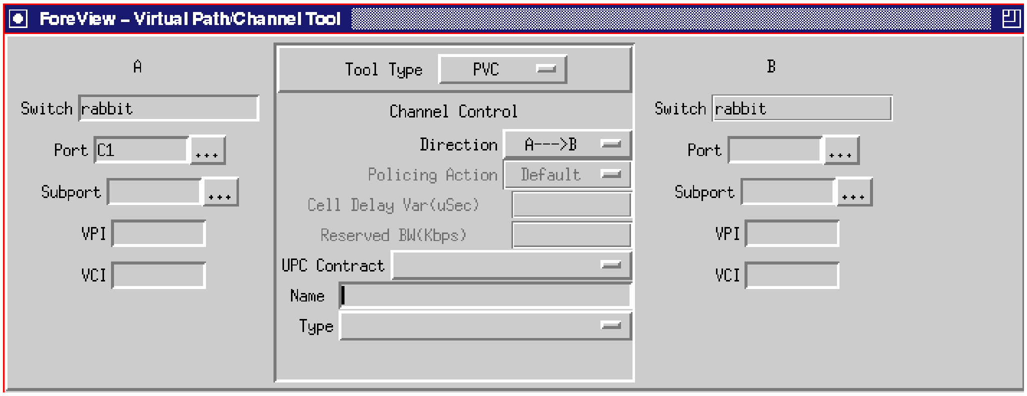
SRTS is only available on unstructured connections. An unstructured service connection is created by specifying all the available timeslots by selecting **`Unchannelized T1`**.

The **`PartialFill`** and **`CAS`** parameters are not applicable to unstructured mode.

Structured mode is selected by indicating the exact timeslots to be used. For example, timeslots 1, 2, and 3 would be selected with the mouse (green indicating a positive selection).

9.4 PVC Tool

Select tool type PVC to browse, create, modify, and delete PVCs (permanent virtual channels). PVCs “ride” inside of virtual paths to create a single virtual connection between two endpoints. Figure 9.5 shows the PVC tool dialog.


ForeView – Virtual Path/Channel Tool

A

Switch rabbit

Port C1

Tool Type PVC

Channel Control

Direction A--->B

Policing Action Default

B

Switch rabbit

Figure 9.5 - PVC Tool Dialog

9.4.1 Key Fields for the PVC Tool

These fields are filled in automatically when an existing path or circuit is chosen using the browser. The key control fields for the PVC tool are defined as follows:

Switch A and B

Port The number of the port where the circuit enters/exits the switch.

Subport Launches the sub-port timeslot configuration dialog. This configuration option is available only when selecting ports from FORE Systems’ Circuit Emulation Services (CES) DS1 and E1 network modules.

NOTE

For information on the sub-port timeslot configuration dialog for CES network modules, see ”CES Configuration for Smart PVCs” on page 9-14.

VPI The Virtual Path Identifier (VPI) on which the circuit enters / exits the switch.

VCI The Virtual Channel Identifier (VCI) on which the circuit enters / exits the switch.

NOTE For PVCs, switch B must be the same as switch A. The Switch B field is read-only.

Direction Toggled selection for PVC creation. Choices are bi-directional (<-->), and uni-directional (--> or <--). The default value is bi-directional.

9.4.2 Optional Fields for the PVC Tool

The optional control fields for the PVC tool are defined as follows:

Policing Action Choices are “default”, “tag”, or “drop”. Default uses the switch default policing action in the SNMP variable swBoardPolicingAction. This variable can be modified via AMI. Tag will cause the CLPI bit within cells that violate the bandwidth level. Drop will discard cells that violate bandwidth level.

Cell Delay Var (uSec) Indicates the default value for the Cell Delay Variation Tolerance (CDVT) setting. The default setting is 1,000 microseconds.

Reserved BW (Kbps) The amount of peak reserved bandwidth for the circuit or path in kilobits per second.

NOTE For switches running *ForeThought* software versions 3.4 or later, the Policing Action, Cell Delay Variation, and Reserved Bandwidth functionality is incorporated into the UPC Contract option.

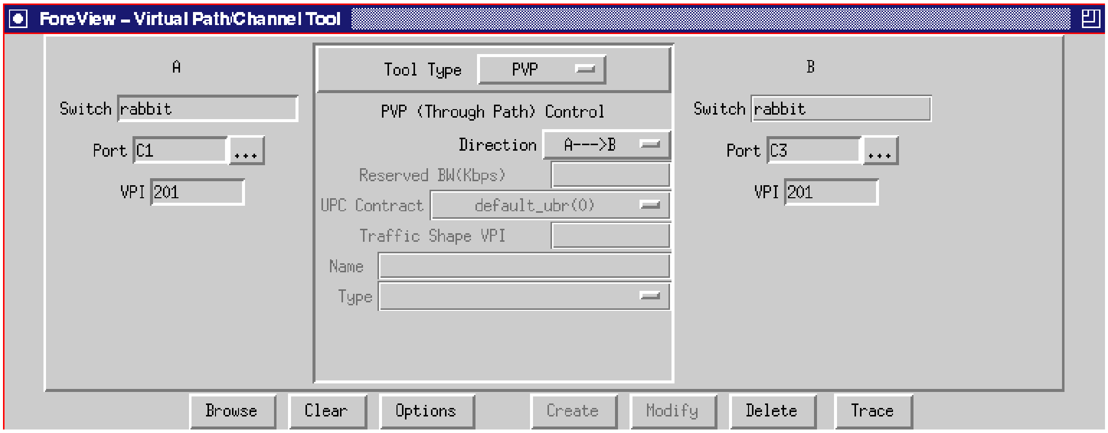
UPC Contract A method of establishing traffic bandwidth contracts for cells entering a switch. Those cells that exceed the specified contract are “tagged” or “dropped,” depending on what is defined in the contract. This option is implemented in *ForeThought* software versions 3.4 and later.

Name Indicates the name you want to assign to this channel to help identify it uniquely. It is most useful for billing purposes so you can identify which channels are being used by which customers. Can be up to 32 ASCII characters long.

Type Indicates the connection type for the endpoints of this path with respect to a particular network. **Orig** (originating) means that the ingress/egress endpoint of the path is connected to the source node which is outside the network. **Tran** (transitional) means that the ingress/egress endpoint of the path is connected to a node within the network. **Term** (terminating) means that the ingress/egress endpoint of the path is connected to the destination node which is outside the network. When appended with **P** or **MP**, this label is further defined as being a point-to-point, point-to-multipoint, multipoint-to-point, or multipoint-to-multipoint. For example, **OrigP, OrigMP, TranP, TranMP,** etc.

9.5 PVP Tool

Select tool type PVP to browse, create, and delete through paths. Figure 9.6 shows the PVP tool dialog.


ForeView – Virtual Path/Channel Tool

Tool Type: PVP

A
Switch: rabbit
Port: C1
VPI: 201

PVP (Through Path) Control
Direction: A--->B
Reserved BW(Kbps):
UPC Contract: default_ubr(0)
Traffic Shape VPI:
Name:
Type:

B
Switch: rabbit
Port: C3
VPI: 201

Figure 9.6 - PVP Tool Dialog

9.5.1 Key Fields for the PVP Tool

These fields are filled in automatically when an existing path or circuit is chosen using the browser. The key control fields for the PVP tool are defined as follows:

Switch A and B

Port The number of the port where the path enters/exits the switch.

VPI The Virtual Path Identifier (VPI) on which the path enters/exits the switch.

Direction Toggled selection for path creation. Choices are bi-directional (<-->), and uni-directional (--> or <--). The default value is bi-directional.

9.5.2 Optional Fields for the PVP Tool

The optional control fields for the PVP tool are defined as follows:

Reserved BW (Kbps) The amount of peak reserved bandwidth for the circuit or path in kilobits per second.

UPC Contract Toggled variable to select a UPC contract or clear a contract that has been selected. When selecting a contract, the UPC configuration dialog is launched.

Traffic Shape VPI Indicates the incoming VPI for this through path. When the traffic shaping port is not the port connected to the WAN, a through path must be created from the WAN port to the traffic shaping port. Cells arrive from the network at the traffic shaping port with this value equal to the VPI of the terminating path at the traffic shaping port.

NOTE

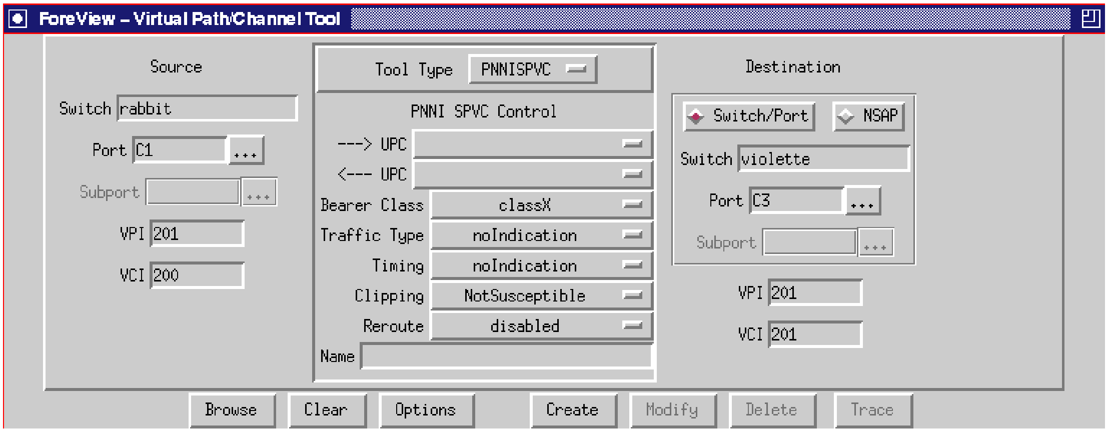
If you want to shape traffic on more than two ports on a given network module, it is recommended that you set the traffic memory model to model number 5 for that network module.

Name Indicates the name you want to assign to this channel to help identify it uniquely. It is most useful for billing purposes so you can identify which channels are being used by which customers. Can be up to 32 ASCII characters long.

Type Indicates the connection type for the endpoints of this path with respect to a particular network. **`Orig`** (originating) means that the ingress/egress endpoint of the path is connected to the source node which is outside the network. **`Tran`** (transitional) means that the ingress/egress endpoint of the path is connected to a node within the network. **`Term`** (terminating) means that the ingress/egress endpoint of the path is connected to the destination node which is outside the network. When appended with **`P`** or **`MP`**, this label is further defined as being a point-to-point, point-to-multipoint, multipoint-to-point, or multipoint-to-multipoint. For example, **`OrigP, OrigMP, TranP, TranMP,`** etc.

9.6 PNNI SPVC Tool

Select tool type PNNISPVC to browse, create, and delete PNNI Smart PVCs. This tool allows you to configure *ForeThought* PNNI SPVCs. Unlike the SPANS SPVCs, PNNI SPVCs are inherently bidirectional, which means that a single signalling call establishes the circuits in both directions. Although PNNI SPVCs are bidirectional, the endpoint that initiates the call setup is known as the source and the other endpoint is known as the destination. Figure 9.7 shows the PNNI SPVC tool dialog.



ForeView – Virtual Path/Channel Tool

Source

Switch rabbit

Port C1

Subport

VPI 201

VCI 200

Tool Type PNNISPVC

PNNI SPVC Control

---> UPC

<--- UPC

Bearer Class classX

Traffic Type noIndication

Timing noIndication

Clipping NotSusceptible

Reroute disabled

Name

Destination

● Switch/Port ○ NSAP

Switch violette

Port C3

Subport

VPI 201

VCI 201

Figure 9.7 - PNNI SPVC Tool Dialog

9.6.1 Key Fields for the PNNI SPVC Tool

These fields are filled in automatically when an existing path or circuit is chosen using the browser. For manual configuration of *ForeThought* PNNI SPVCs, entries can be made in the following fields:

Source Switch Shows the switch name of the local switch fabric for this PNNI SPVC.

Source Port Shows the port number on the local switch fabric for this PNNI SPVC.

Source Subport Launches the sub-port timeslot configuration dialog. This configuration option is available only when selecting ports from FORE Systems' Circuit Emulation Services (CES) DS1 and E1 network modules.

NOTE For information on the sub-port timeslot configuration dialog for CES network modules, see ”CES Configuration for Smart PVCs” on page 9-14.

Source VPI Shows the virtual path number on the local switch fabric for this PNNI SPVC.

Source VCI Shows the virtual channel number on the local switch fabric for this PNNI SPVC.

Destination Switch/Port Click this button to specify a destination switch and port. Use this option if the destination switch is a FORE Systems switch. The tool will retrieve the NSAP prefix automatically.

Destination NSAP Click this button to specify a destination NSAP address.

Destination Switch Enter the switch name of the remote switch fabric for this PNNI SPVC.

Destination Port Select the port number of this terminating PNNI SPVC at the destination end.

Destination VPI Enter the virtual path number on the destination switch fabric for this PNNI SPVC.

Destination VCI Enter the virtual channel number on the destination switch fabric for this PNNI SPVC.

9.6.2 Optional Fields for the PNNI SPVC Tool

The optional control fields for the PNNI SPVC tool are defined as follows:

---> (Source) UPC Displays the forward (going from the local switch fabric to the remote switch fabric) UPC contract index associated with this SPVC.

<--- (Destination) UPC Shows the backward (going from the remote switch fabric to the local switch fabric) UPC contract index associated with this SPVC.

Bearer Class Selects the broadband bearer class specified for this SPVC. Options are **classA**, **classC**, or **classX**.

Traffic Type Selects the requested broadband bearer traffic type for this SPVC. Options are **noIndication**, **cbr**, or **vbr**.

Timing Selects the broadband bearer timing requirements for this SPVC. Options are **`noIndication`**, **`end2endRequired`** (end-to-end timing is required), or **`end2endNotReqd`** (end-to-end timing is not required).

Clipping During speech transmission, clipping is the loss of a brief interval at the beginning of a speech spurt. Using **`NotSusceptible`** indicates this SPVC is not susceptible to clipping. Using **`Susceptible`** indicates this SPVC is susceptible to clipping. The default is **`NotSusceptible`**.

Reroute Enabled indicates that this SPVC will be examined to see if it is using a sub-optimal route. If it is, it will be rerouted according to the parameters in conf spvc pnni parameters reroute. Disabled indicates that this SPVC will not be examined to see if it is using a sub-optimal route. The default state for PNNI SPVCs is disabled. If you want to change this value for this PNNI SPVC after you create it, you must delete it and then recreate it.

Name Indicates the name you want to assign to this UNI to help identify it uniquely. It is most useful for billing purposes so you can identify which channels are being used by which customers. Can be up to 32 ASCII characters long.

9.7 Incoming Path Tool

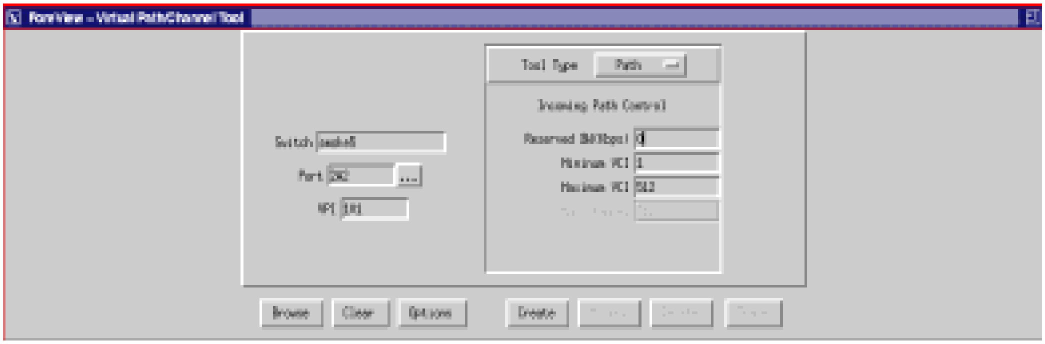
Outgoing (originating) and incoming (terminating) paths are points at which a virtual path originates and terminates. They are also referred to as virtual path terminators. For example, if a virtual path exists from switch A to switch B, then there must be an outgoing path on switch A and an incoming path on switch B.

An incoming path is defined by the parameters: input path (VPI) and input port. Outgoing and incoming paths are the endpoints of virtual paths and are used primarily for bandwidth allocation. Outgoing and incoming paths are automatically allocated by the Virtual Path/Channel Tool when a PVC is created using the PVC tool.

NOTE

The bandwidth allocated to outgoing and incoming paths is used to control the amount of bandwidth entering or leaving a virtual path. The total bandwidth used by virtual channels on an outgoing path or an incoming path cannot exceed the amount of bandwidth allocated to that path.

When you attempt to create a PVC with no corresponding incoming and outgoing paths, the Virtual Path/Channel Tool prompts you to create the paths. Select tool type Path to browse, create, modify, and delete incoming paths of PVCs. An incoming path is the point at which a virtual path terminates. Figure 9.8 shows the Incoming Path tool dialog



ForeView - Virtual Path/Channel Tool

Tool Type: Path

Incoming Path Control

Switch: sasha5

Port: 2A2

VPI: 101

Reserved BW(Kbps): 0

Minimum VCI: 1

Maximum VCI: 512

Figure 9.8 - Incoming Path Tool Dialog

9.7.1 Key Fields for the Incoming Path Tool

These fields may be filled in automatically when an existing path is chosen using the browser. For manual configuration of incoming paths, entries can be made in the following fields:

Switch Shows the switch name of the terminating switch fabric for this path.

Port Shows the port number on the terminating switch fabric.

VPI Shows the virtual path number on the terminating switch fabric.

9.7.2 Optional Fields for the Incoming Path Tool

Reserved BW (Kbps) Indicates the amount of bandwidth, specified in Kbps, that you want to reserve on this incoming (or terminating) path.

Minimum VCI Indicates the bottom number for the range of VCIs that are reserved for VCCs on this incoming virtual path terminator. The default is **1**.

Maximum VCI Indicates the top number for the range of VCIs that are reserved for VCCs on this incoming virtual path terminator. The default is **512**.

Max Channels Indicates the maximum number of VCCs that can be created on this incoming virtual path terminator. The allowable maximum is **512**.

9.8 Outgoing Path Tool

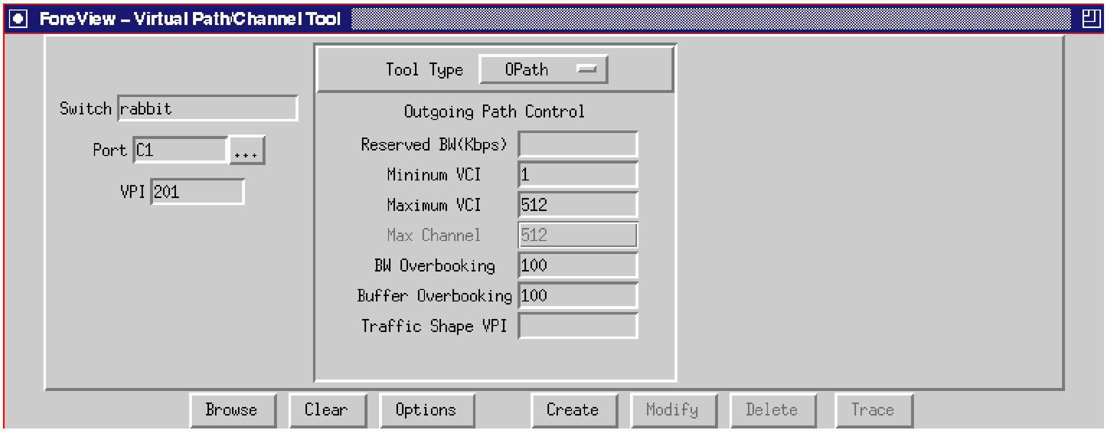
As previously stated, outgoing (originating) and incoming (terminating) paths are points at which a virtual path originates and terminates. For example, if a virtual path exists from switch A to switch B, then there must be an outgoing path on switch A and an incoming path on switch B.

An outgoing path is defined by two parameters: output path and output port. Outgoing and incoming paths are the endpoints of virtual paths and are used primarily for bandwidth allocation. Outgoing and incoming paths are automatically allocated by the Virtual Path/Channel Tool when a PVC is created using the PVC tool.

NOTE

The bandwidth allocated to outgoing and incoming paths is used to control the amount of bandwidth entering or leaving a virtual path. The total bandwidth used by virtual channels on an outgoing path or an incoming path cannot exceed the amount of bandwidth allocated to that path.

When you attempt to create a PVC with no corresponding incoming and outgoing paths, the Virtual Path/Channel Tool prompts you to create the paths. Select tool type OPath to browse, create, modify, and delete outgoing paths of PVCs. An outgoing path is the point at which a virtual path originates. Figure 9.9 shows the Outgoing Path tool dialog



Switch rabbit

Port C1

VPI 201

Tool Type OPath

Outgoing Path Control

Reserved BW(Kbps)

Mininum VCI 1

Maximum VCI 512

Max Channel 512

BW Overbooking 100

Buffer Overbooking 100

Traffic Shape VPI

Figure 9.9 - Outgoing Path Tool Dialog

9.8.1 Key Fields for the Outgoing Path Tool

These fields may be filled in automatically when an existing path is chosen using the browser. For manual configuration of outgoing paths, entries can be made in the following fields:

Switch Shows the switch name of the originating switch fabric for this path.

Port Shows the port number on the originating switch fabric.

VPI Shows the virtual path number on the originating switch fabric.

9.8.2 Optional Fields for the Incoming Path Tool

Reserved BW (Kbps) Indicates the amount of bandwidth, specified in Kbps, that you want to reserve on this outgoing (or originating) path.

Max Channels Indicates the maximum number of channels that can be created on this outgoing (or originating) path.

Minimum VCI Indicates the bottom number for the range of VCIs that are reserved for VCCs on this outgoing virtual path terminator. The default is **`1`**.

Maximum VCI Indicates the top number for the range of VCIs that are reserved for VCCs on this outgoing virtual path terminator. The default is **`512`**.

BW Overbooking Indicates the bandwidth overbooking level assigned to this outgoing path, specified as a percentage. Enter an integer value from **`1`** to **`500`**. The default is **`100`**, which means that no overbooking has been defined. Values less than **`100`** cause underbooking. Values greater than **`100`** denote overbooking.

Buffer Overbooking Indicates the buffer overbooking level assigned to this outgoing path, specified as a percentage. Enter an integer value greater than or equal to **`1`**. The default is **`100`**, which means that no overbooking has been defined. Values less than **`100`** cause underbooking. Values greater than **`100`** denote overbooking.

Traffic Shape VPI Sets the output port of a traffic shaping originating VPI. Setting this value configures traffic shaping on the originating path. Cells bound for the network leave the traffic shaping port with this VPI. When the traffic shaping port is the WAN port, this value equals the input VPI of the originating path. If the traffic shaping port is not the WAN port, this value equals the input VPI of the through path from the shaping port to the WAN port.

9.9 Signalling Path Tool

The Virtual Path/Channel Tool tool provides the means to browse, create, modify, and delete SPANS (Simple Protocol for ATM Network Signalling) and UNI 3.x signalling paths on a given VPI for a selected switch. Simply select tool type SigPath; select a switch; determine the port, and VPI; then determine the signalling path type (SPANS or UNI 3.x).

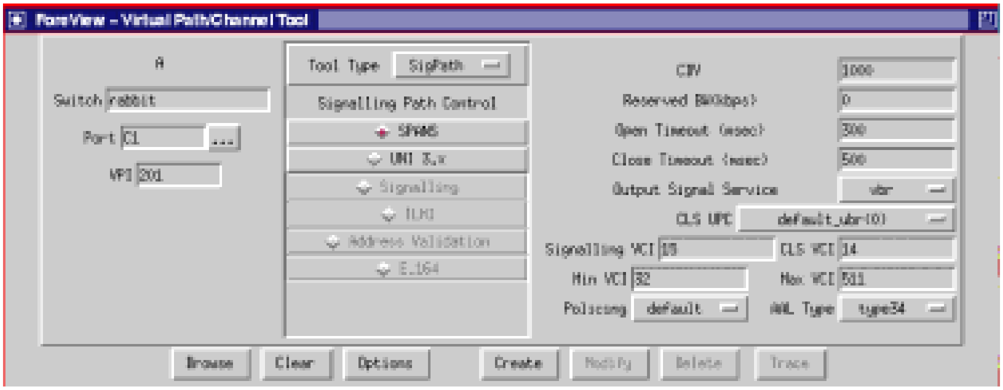
SPANS is FORE Systems' proprietary signalling protocol used for establishing SVCs between other FORE Systems equipment. In an SVC environment, ATM virtual channel connections (VCCs) are dynamically established and released as needed using the SPANS call/connection control signalling protocol, which operates between ATM endsystems and the FORE ATM network.

ForeRunner switches are also compatible with ATM networks that conform to the ATM Forum UNI Specification Version 3.x. The signalling entities use the UNI 3.x signalling protocol to establish and release calls (association between ATM endpoints) and connections (VCCs). Signalling procedures include the use of addressing to locate ATM endpoints and allocation of resources in the network for the connection. It also provides indication and negotiation between ATM endpoints for selection of end-to-end protocols and their parameters.

The following sections explain the SigPath fields and their values for SPANS and UNI 3.x signalling.

9.9.1 SPANS Configuration

To browse, create, and delete SPANS signalling paths on a given VCI for a selected switch, select SPANS for the Signalling Path Control; select a switch; determine the port and VPI; then determine whether the default parameters are adequate. Figure 9.10 shows an example of the SPANS configuration dialog.



A

Switch: rabbit

Port: C1 ...

VPI: 201

Tool Type: SigPath

Signalling Path Control

● SPANS

○ UNI 3.x

○ Signalling

○ ILMI

○ Address Validation

○ E.164

CBV: 1000

Reserved BW(kbps): 0

Open Timeout (msec): 300

Close Timeout (msec): 500

Output Signal Service: ubr

CLS UPC: default_ubr(0)

Signalling VCI: 15

CLS VCI: 14

Min VCI: 32

Max VCI: 511

Policing: default

AAL Type: type34

Figure 9.10 - Signalling Path Tool Dialog for SPANS

9.9.1.1 Key Fields for the SPANS Signalling Path Tool

These fields are filled in automatically when an existing path or circuit is chosen using the browser. For manual creation of signalling paths, entries for SPANS can be made in the following fields:

Switch A The name of the switch from which the signalling path is originating. A switch can be selected from a map, or a switch name can be entered in this field.

Port Indicates the port number on which the SPANS signalling path is to be created.

VPI Indicates the number of the SPANS path that is to be created.

NOTE

Before a SPANS signalling path can be created on a given VPI, an originating and a terminating path must exist for that same VPI.

9.9.1.2 Optional Fields for the SPANS Signalling Path Tool

CDV Indicates the Cell Delay Variation Tolerance (CDVT) associated with the peak cell rates in microseconds for the Signalling VCI.

Reserved BW (kbps) Indicates the amount of bandwidth to be reserved on the VCI for SPANS signalling messages.

Open Timeout (msec) The timeout for SPANS open requests. This option should be used on links that have a high propagation delay, such as satellite links. The default is 300 msec.

Close Timeout (msec) The timeout for SPANS close requests. This option should be used on links that have a high propagation delay, such as satellite links. The default is 500 msec.

Output Signal Service Configures the SPANS signalling channel to be put into either the UBR or VBR queue on the output side at the time the SPANS channel is created. By putting the SPANS signalling channel in the VBR queue, the SPANS signalling messages receive higher priority on the output side. This keeps UBR traffic from congesting the signalling traffic. The default is vbr.

CLS UPC A method of establishing traffic bandwidth contracts for cells entering a switch. Those cells that exceed the specified contract are “tagged” or “dropped,” depending on what is defined in the contract. This option is implemented in *ForeThought* software versions 3.4 and later and applies to the CLS VCI. If no index is specified, then no traffic policing will take place on the connectionless VCI. It is assigned a UPC index of 0, and all traffic on this VCI is treated as UBR traffic. This is the default.

Signalling VCI Indicates the VCI to use for SPANS signalling messages. The default is 15.

CLS VCI Indicates the VCI to use for connectionless messages. The default is 14.

Min VCI Indicates the bottom number for the range of VCIs to be reserved for SPANS SVCs on this path. The default is **32**. You can change this range if you want to limit the number of SVCs on this path, limit the number of SPANS SVCs with respect to UNI SVCs, or divide the VCI range into a region reserved for SPANS SVCs and a region reserved for UNI SVCs.

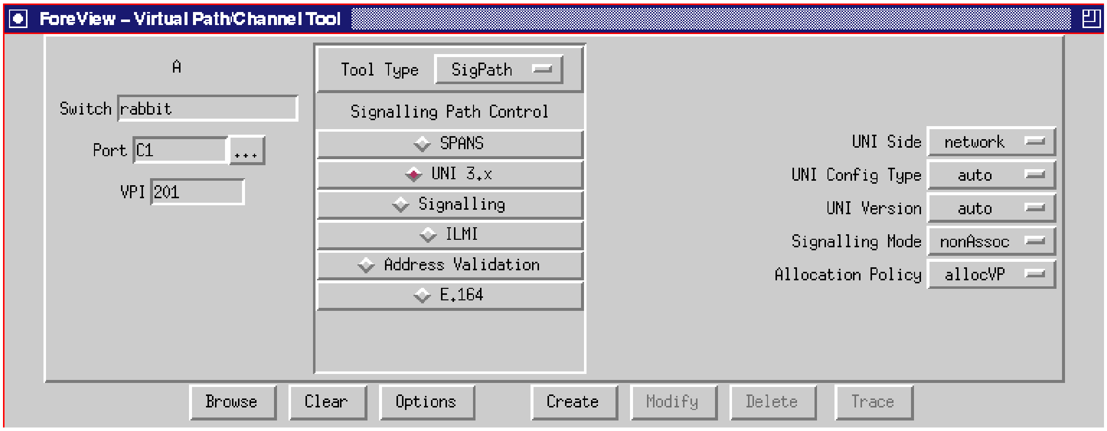
Max VCI Indicates the top number for the range of VCIs to be reserved for SPANS SVCs on this path. The default is the maximum number of VCIs that the path supports. You can change this range if you want to limit the number of SVCs on this path, limit the number of SPANS SVCs with respect to UNI SVCs, or divide the VCI range into a region reserved for SPANS SVCs and a region reserved for UNI SVCs.

Policing Choices are “default”, “tag”, or “drop”. Default uses the switch default policing action in the SNMP variable swBoardPolicingAction. This variable can be modified via AMI. Tag will cause the CLPI bit within cells that violate the bandwidth level. Drop will discard cells that violate bandwidth level. This applies to the Signalling VCI.

AAL Type AAL (ATM Adaptation Layer) divides the user information into segments suitable for packaging into a series of ATM cells. There are several types of AALs in use. FORE Systems currently supports AAL5 and AAL3/4. AAL3/4 supports connection-oriented VBR data transfer and connectionless VBR data transfer, respectively. AAL5 is defined as Simple and Efficient Adaptation Layer (SEAL). This applies to the Signalling VCI.

9.9.2 UNI 3.x Configuration

To browse, create, modify, and delete UNI 3.x signalling paths on a given VPI for a selected switch, select UNI 3.x for the Signalling Path Control; select a switch; determine the port, VPI, and VCI; then determine whether the default parameters are adequate. Figure 9.11 shows an example of the UNI 3.x configuration dialog.



ForeView – Virtual Path/Channel Tool

A

Switch rabbit

Port C1 ...

VPI 201

Tool Type SigPath

Signalling Path Control

◇ SPANS

◆ UNI 3.x

◇ Signalling

◇ ILMI

◇ Address Validation

◇ E.164

UNI Side network

UNI Config Type auto

UNI Version auto

Signalling Mode nonAssoc

Allocation Policy allocVP

Figure 9.11 - Signalling Path Tool Dialog for UNI 3.x

9.9.2.1 Key Fields for the UNI 3.x Path Tool

These fields are filled in automatically when an existing path or circuit is chosen using the browser. For manual creation of UNI 3.x signalling paths, entries can be made in the following fields:

Switch A The name of the switch from which the signalling path is originating. A switch can be selected from a map, or a switch name can be entered in this field.

Port The number of the port where the circuit enters the switch.

VPI The Virtual Path Identifier (VPI) on which the circuit enters the switch.

NOTE

Before a UNI signalling path can be created on a given VPI, an originating and a terminating path must exist for that same VPI.

9.9.2.2 Optional Fields for the UNI 3.x Path Tool

UNI Side Indicates the switch user side or network side. If the connection is to a host, choose network. If the connection is to another switch, one switch must be user and the other switch must be network.

UNI Config Type Indicates the configuration type. PublicUNI means that this link will be used between this switch and a public switch. Auto means that the operation type will be determined dynamically. IISP is used for switch-to-switch signalling. This is used for static NNI routes. The default is auto.

UNI Version The version of the UNI protocol to use at initialization. auto means that the UNI attempts to determine automatically which version of the UNI protocol to use. uni30 means that this link uses version 30 of the UNI protocol. uni31 means that this link uses version 31 of the UNI protocol. pnni means ??.

Signalling Mode Shows the mode to be used for signalling. If set to **nonAssoc** (Non-associated signalling), the UNI encodes the connection identifier with Non-associated signalling bits. If set to **vpAssoc** (VP-associated signalling), the UNI encodes the connection identifier with the VP-associated signalling bits. The default is **nonAssoc**.

Allocation Policy Shows the allocation policy for a network side UNI. If set to **vp**, the network side UNI allocates connections in its containing VP only. If set to **allocLink**, the UNI allocates connections in its containing VP and may allocate connections in other VPs that are available to it. The default is **vp**.

NOTE

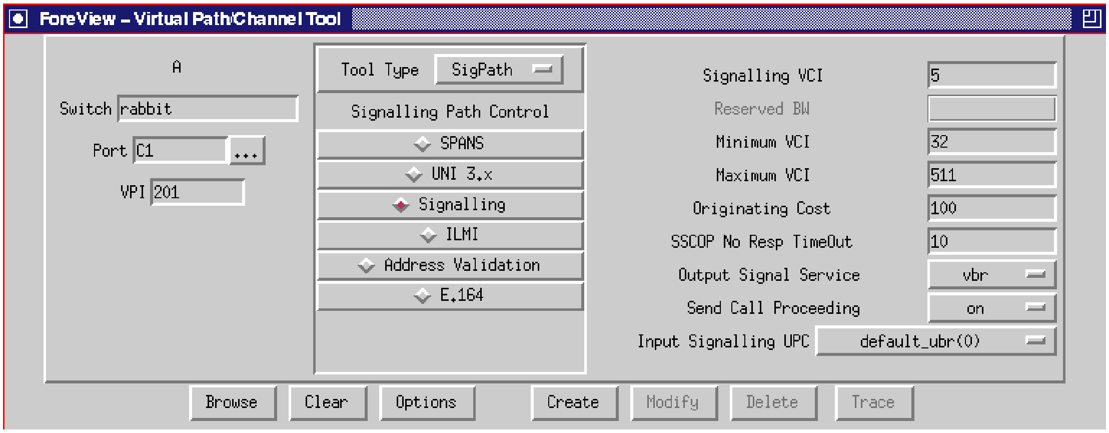
Click on the Signalling button to configure the VCI used for the UNI 3.x signalling messages, bandwidth, AAL type, and the minimum and maximum VCI values.

NOTE

Click on the ILMI button to configure to enable ILMI NSAP registration for this port (only when a host is connected).

9.9.3 UNI 3.x Signalling Configuration

As an extension to the UNI 3.x signalling path tool, click on the Signalling button (this button is active only when UNI 3.x is selected from the tool) to configure the signalling VCI. Figure 9.12 shows an example of the UNI 3.x signalling dialog.



Switch rabbit

Port C1

VPI 201

Tool Type SigPath

Signalling VCI 5

Reserved BW

Minimum VCI 32

Maximum VCI 511

Originating Cost 100

SSCOP No Resp TimeOut 10

Output Signal Service vbr

Send Call Proceeding on

Input Signalling UPC default_ubr(0)

Figure 9.12 - UNI 3.x Signalling Dialog

9.9.3.1 Key Fields for the UNI 3.x Signalling Path Tool

These fields are filled in automatically when an existing path or circuit is chosen using the browser. For manual creation of UNI 3.x signalling paths, entries can be made in the following fields:

Signalling VCI Indicates the VCI to use for the UNI 3.x signalling messages. The default reserved VCI is **5**.

Reserved BW Indicates the amount of bandwidth that will be reserved on the VCI for UNI 3.x signalling messages (VCI 5).

Minimum VCI Indicates the bottom number for the range of VCIs to be reserved for UNI 3.x signalling messages. The default is **32**.

Maximum VCI Indicates the top number for the range of VCIs to be reserved for UNI 3.x signalling messages. The default is **255**.

Originating Cost Shows the cost of each link configured at the originating end of the signalling path.

SSCOP No Resp TimeOut The value to be set for the duration of the SSCOP no response timer. This is the time in seconds to wait before bringing the SSCOP connection down. This parameter can be set to a value higher than the default when the remote host is experiencing a heavy load and cannot process a signalling request in time. The default is 10 seconds for UNI 3.0 and 7 seconds for UNI 3.1.

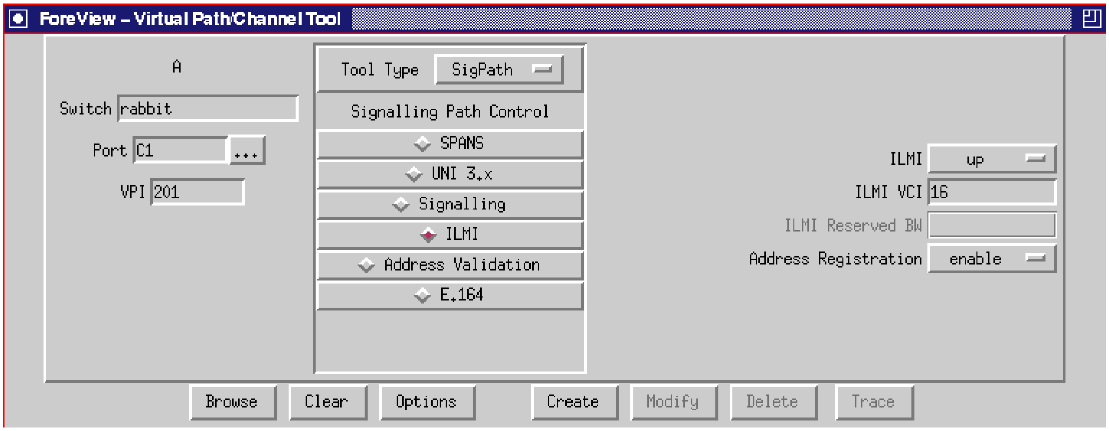
Output Signal Service The service queue into which the output signalling channel should be inserted. Can be VBR or UBR. The default is VBR. By putting the UNI signalling channel in to the VBR queue, the UNI signalling messages receive higher priority on the output side.

Send Call Proceeding On means that the UNI sends call proceeding messages for setup messages that it receives and successfully forwards.

Input Signalling UPC The index number of the UPC traffic contract to be applied to the input signalling channel.

9.9.4 UNI 3.x ILMI Signalling Configuration

As an extension to the UNI 3.x signalling path tool, click on the ILMI button (this button is active only when UNI 3.x is selected from the tool) to configure ILMI signalling VCIs. Figure 9.13 shows an example of the UNI 3.x ILMI configuration dialog.



ForeView – Virtual Path/Channel Tool

A

Switch rabbit

Port C1

VPI 201

Tool Type SigPath

Signalling Path Control

◇ SPANS
◇ UNI 3.x
◇ Signalling
◆ ILMI
◇ Address Validation
◇ E.164

ILMI up

ILMI VCI 16

ILMI Reserved BW

Address Registration enable

Figure 9.13 - Signalling Path Tool Dialog for ILMI

9.9.4.1 Key Fields for the UNI 3.x ILMI Path Tool

These fields are filled in automatically when an existing path or circuit is chosen using the browser. For manual creation of UNI 3.x signalling paths, entries can be made in the following fields:

ILMI Enables ILMI NSAP registration for this port (only when a host is connected). The default is up for UNI 3.x signalling paths.

Before a host can establish connections over a physical interface, the host must know the NSAP address for that interface. The primary purpose of ILMI is to discover and register these NSAP addresses dynamically.

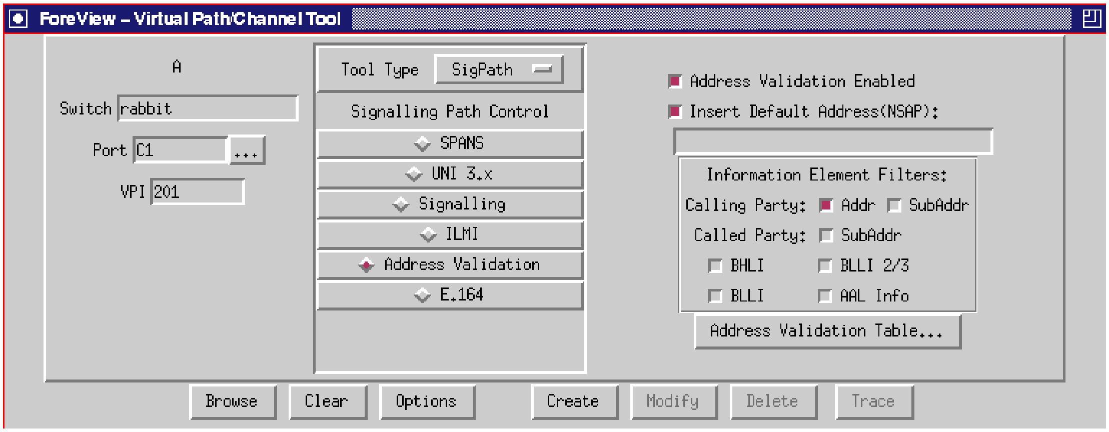
ILMI VCI Indicates the VCI to use for ILMI signalling messages. The default reserved VCI is **16**.

ILMI Reserved BW Indicates the amount of bandwidth that will be reserved on the VCI for ILMI messages (VCI 16).

Address Registration Enables the display of the NSAP addresses of all of the ports on a switch fabric that have been registered via ILMI. ILMI address registration occurs between the switch and host. Valid options are **`enable`**, **`disable`**, and **`ignore`**. When **`ignore`** is selected, the UNI will accept and register addresses through ILMI but will not report these addresses to other UNIs.

9.9.5 UNI 3.x Address Validation

As an extension to the UNI 3.x signalling path tool, click on the Address Validation button (this button is active only when UNI 3.x is selected from the tool) to perform address validation for UNI 3.x signalling paths. Figure 9.14 shows an example of the UNI 3.x Address Validation configuration dialog.



ForeView – Virtual Path/Channel Tool

A

Switch: rabbit

Port: C1

VPI: 201

Tool Type: SigPath

Signalling Path Control

○ SPANS
○ UNI 3.x
○ Signalling
○ ILMI
● Address Validation
○ E.164

☒ Address Validation Enabled

☒ Insert Default Address(NSAP):

Information Element Filters:

Calling Party: ☒ Addr ☐ SubAddr

Called Party: ☐ SubAddr

☐ BHLI ☐ BLLI 2/3

☐ BLLI ☐ AAL Info

Figure 9.14 - Signalling Path Tool Dialog for Address Validation

9.9.5.1 Key Fields for UNI 3.x Signalling Address Validation

These fields may be filled in automatically when an existing path or circuit is chosen using the browser. For manual address validation of UNI 3.x signalling paths, entries can be made in the following fields:

Address Validation Enabled Checking this box enables validation for the NSAP address of a UNI 3.x signalling path.

Insert Default Address (NSAP) The port-based NSAP address of the calling party.

Information Element Filters

Controls the filtering of signalling elements of the UNI 3.x signalling path. Filters can be applied to the following:

Calling Party: Filters the Address and/or Subaddress of the call originating entity.

Called Party: Filters the Subaddress of the called party.

BHLI: Filters the Broadband High Layer Information (BHLI), which provides compatibility checking by an addressed entity (e.g. a recipient of a call).

BLLI: Filters the first Broadband Low Layer Information (BLLI) layer, which provides compatibility checking by an addressed entity. This information is normally transferred transparently between the call originator and the call recipient.

BLLI 2/3: Filters the second and third Broadband Low Layer Information (BLLI) layers.

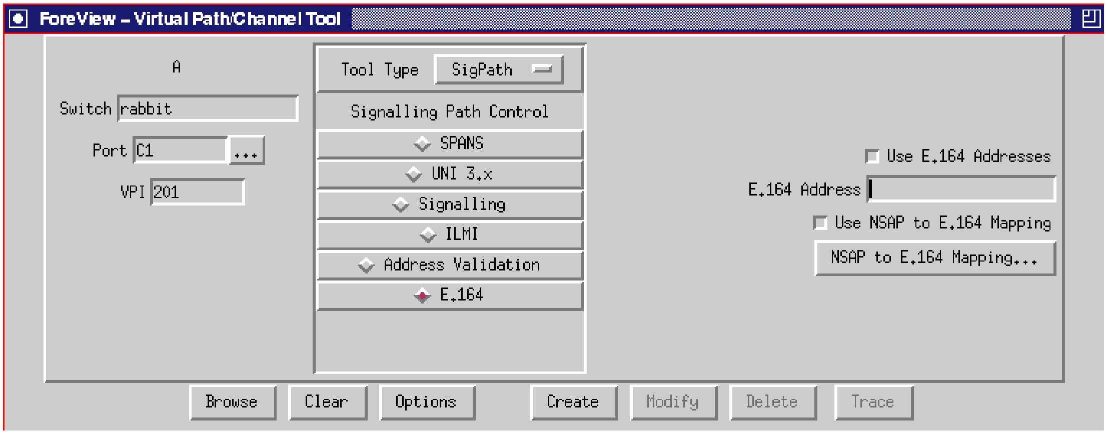
AAL Info: Filters on the AAL (ATM Adaptation Layer) information.

Address Validation Table

Click this button to launch a table of addresses for this UNI. The addresses in this table can be either accepted or rejected. To launch the table, you must provide a switch name, port, and VPI. From the table, you can add and delete addresses requiring validation. You can also update addresses in the table.

9.9.6 UNI 3.x Address Mapping

As an extension to the UNI 3.x signalling path tool, click on the E.164 button (this button is active only when UNI 3.x is selected from the tool) to perform address mapping of private E.164 format addresses to public NSAP addresses. Figure 9.15 shows an example of the E.164 address mapping configuration dialog.



ForeView – Virtual Path/Channel Tool

A

Switch rabbit

Port C1

VPI 201

Tool Type SigPath

☐ Use E.164 Addresses

E.164 Address

☐ Use NSAP to E.164 Mapping

Figure 9.15 - Signalling Path Tool Dialog for E.164 Address Mapping

9.9.6.1 Key Fields for UNI 3.x E.164 Address Mapping

These fields may be filled in automatically when an existing path or circuit is chosen using the browser. For manual address mapping of UNI 3.x signalling paths, entries can be made in the following fields:

Use E.164 Addresses Checking this box enables mapping of E.164 format addresses to the NSAP address of a UNI 3.x signalling path.

E.164 Address The port-based E.164 format address of the calling party.

Use NSAP to E.164 Mapping Click this button to enable the mapping of E.164 addresses to NSAP addresses.

NSAP to E.164 Mapping... Click this button to launch a table of address mappings for this UNI. To launch the table, you must provide a switch name, port, and VPI. From the table, you can add and delete address mappings. You can also update addresses in the table.

9.10 Usage Parameter Control (UPC) Contracts

Usage Parameter Control (UPC), also known as traffic policing, is a method of assessing the cells entering the switch for conformance with pre-established traffic contracts. Those cells that exceed the specified contract are “tagged” or “dropped,” depending on what is defined in the contract. This section describes the enhanced traffic management features being incorporated into FORE Systems’ switches. These features permit per-connection as well as per-port/ per-class traffic management, which could be configured via an ATM switch Front Panel.

9.10.1 Traffic Types

Quality of Service (QOS) Management is based on the bandwidth parameters associated with a virtual connection and the class of service and ATM Adaptation Layer (AAL) used for that connection. In order to support voice, video, and data, the ATM Forum has defined three classes of service, or traffic types: Constant Bit Rate (CBR), Variable Bit Rate (VBR), and Unspecified Bit Rate (UBR).

- At connection set-up time, traffic that uses a CBR parameter, such as a voice signal, makes a request for a dedicated Peak Cell Rate (PCR). Once the PCR is defined, the ATM network must be able to guarantee that amount of bandwidth for the duration of the connection.
- At connection set-up time, traffic that uses a VBR parameter, such as a video and data, makes a request for a dedicated PCR, Sustainable Cell Rate (SCR), and Maximum Burst Size (MBS). Once these cell rates are defined, the ATM network must be able to guarantee these rates for the duration of the connection.
- UBR traffic, such as broadcast information and ARP messages, is also known as “best effort” service. UBR provides no bandwidth guarantees.

Because ATM is designed to provide a single network to transport this variety of traffic classes, FORE’s traffic policing and Connection Admission Control (CAC) schemes are vital to allowing this mix of traffic to flow smoothly.

The new traffic management features provided with this release are as follows:

- Provisionable GCRA policing: this feature allows users to control traditional traffic policing on a per-port/per-class and per-connection basis.
- Provisionable AAL5 partial packet policing: this feature allows users to enable and disable AAL5 specific policing on a per-port/per-class and per-connection basis.
- Provisionable UBR tagging: this feature allows users to enable and disable the setting CLP=1 (tagging) of all cells of UBR connections on a per-port and per-connection basis.

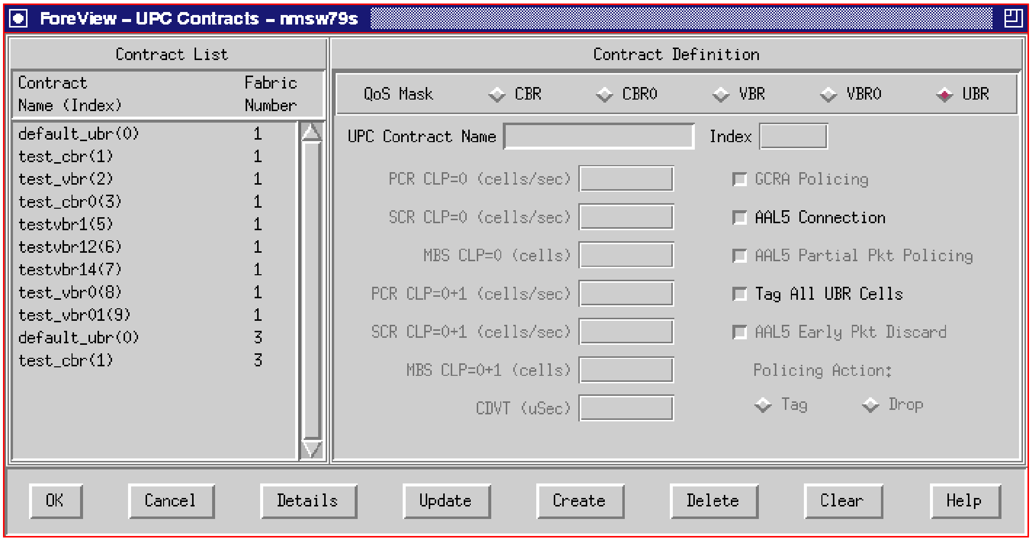
- Provisionable AAL5 packet discard: this feature allows users to enable and disable AAL5 specific packet discard at the egress ports on a per-port/per-class and per-connection basis.

You can launch the main UPC Contracts dialog from either the Front Panel application or the Virtual Path/Channel Tool. From this dialog you can select, create, or delete UPC contracts. The dialog expands to allow you to view all of the existing contracts on all fabrics within an enclosure. This dialog shows the details of each existing contract and is opened by selecting the **`Details`** button.

An example of the UPC Contracts dialog is shown in Figure 9.16 below.

NOTE

When first opened, the cell rate and CDVT entry fields are blank while the traffic management option menu buttons are set to default values. This dialog can be used to create or delete contracts and view contract definitions.



Contract Name (Index)	Fabric Number
default_ubr(0)	1
test_cbr(1)	1
test_vbr(2)	1
test_cbr0(3)	1
testvbr1(5)	1
testvbr12(6)	1
testvbr14(7)	1
test_vbr0(8)	1
test_vbr01(9)	1
default_ubr(0)	3
test_cbr(1)	3

QoS Mask ◇ CBR ◇ CBR0 ◇ VBR ◇ VBR0 ◆ UBR

UPC Contract Name Index

PCR CLP=0 (cells/sec)

SCR CLP=0 (cells/sec)

MBS CLP=0 (cells)

PCR CLP=0+1 (cells/sec)

SCR CLP=0+1 (cells/sec)

MBS CLP=0+1 (cells)

CDVT (uSec)

□ GCRA Policing

□ AAL5 Connection

□ AAL5 Partial Pkt Policing

□ Tag All UBR Cells

□ AAL5 Early Pkt Discard

Policing Action:

◇ Tag ◇ Drop

Figure 9.16 - UPC Contracts Dialog

The UPC Contracts dialog is divided into three areas: the Contract List to the left; the Contract Definition to the right; and the control buttons at the bottom of the dialog. The Contract List is a summary of contracts available from the enclosure. This scrollable list is sorted by fabric number and displays the following information:

Contract Name (Index) Shows the user-defined name associated with this UPC traffic contract and the contract index number. The contract index number corresponds to the UPC index number on the AMI and is a unique number which identifies a specific UPC contract. Different contracts which have the same name are differentiated by their index.

Fabric Number Identifies the fabric on which the contract exists.

Clicking on an entry in the scrollable list causes the details of that contract to be displayed in the Contract Definition area to the right, which displays the following information:

QoS Mask These radio buttons allow you to select the type of traffic this contract defines. The available selections are: CBR, CBR0, VBR, VBR0, and UBR. Upon selection of a QoS mask, the relevant entry fields and menu buttons in the contracts definition area are enabled, while the irrelevant ones are disabled and greyed out. Selecting a QoS mask provides you with a predefined contract template for the given traffic class (eg CBR or VBR0). Changing a QoS mask clears all user editable fields and sets the traffic management options back to their default values.

UPC Contract Name Allows you to give a contract a meaningful 20 character name. The same name can be used for more than one contract.

Index: A read-only field automatically generated by the software. The value is identical to the UPC index value on the switch AMI interface.

PCR CLP=0 (cells/sec) Measures the Peak Cell Rate (PCR) for cells with CLP=0.

SCR CLP=0 (cells/sec) Measures the Sustained Cell Rate (SCR) for cells with CLP=0.

MBS CLP=0 (cells) Measures the Maximum Burst Size (MBS), which is the maximum amount of cells that can be transmitted at the PCR.

PCR CLP=0+1 (cells/sec) Indicates the Peak Cell Rate (PCR), specified in cells / sec, for all cells.

SCR CLP=0+1 (cells/sec) Indicates the Sustainable Cell Rate (SCR), specified in cells / sec, for all cells.

MBS CLP=0+1 (cells) Indicates the Maximum Burst Size (MBS), specified in cells, for all cells.

CDVT (uSec) Indicates the Cell Delay Variation Tolerance (CDVT) associated with the peak cell rates, specified in microseconds. If the CDVT is not specified here, the default CDVT value associated with the port will be used.

GCRA Policing The GCRA Policing Status menu button either enables or disables traditional GCRA traffic policing for any connection using this contract. The default status value is ‘enabled’ for connections other than UBR connections which have policing ‘disabled’.

AAL5 Connection The AAL5 Connection menu button allows the operator to specify whether the connection that will use this contract is an AAL5 connection or not. The default value is ‘not AAL5’.

The AAL5 Partial Pkt Policing This menu button is used to either enable or disable partial packet policing on ingress AAL5 traffic. This option is meaningful, and therefore this button is active, only if GCRA policing is enabled and the connection is AAL5. The default value is ‘no Partial Packet Policing’.

Tag All UBR Cells The Tag All UBR Cells menu button is to either enable or disable tagging of all UBR traffic cells. The default value is ‘no Tagging’.

AAL5 Early Packet Discard The AAL5 Early Packet Discard menu button is to either enable or disable the early packet discard functionality for egress AAL5 traffic cells. This button is active only if the connection is an AAL5 connection. The default value is ‘enabled’.

Policing Action The Policing Action menu selection has two radio buttons allowing you to select either the Tag or Drop action on non-conforming cells. For contracts which allow the operator to specify a Tag action, this button is activated only if GCRA policing is enabled. The default value is ‘Drop’.

9.10.2 Detailed UPC Reference

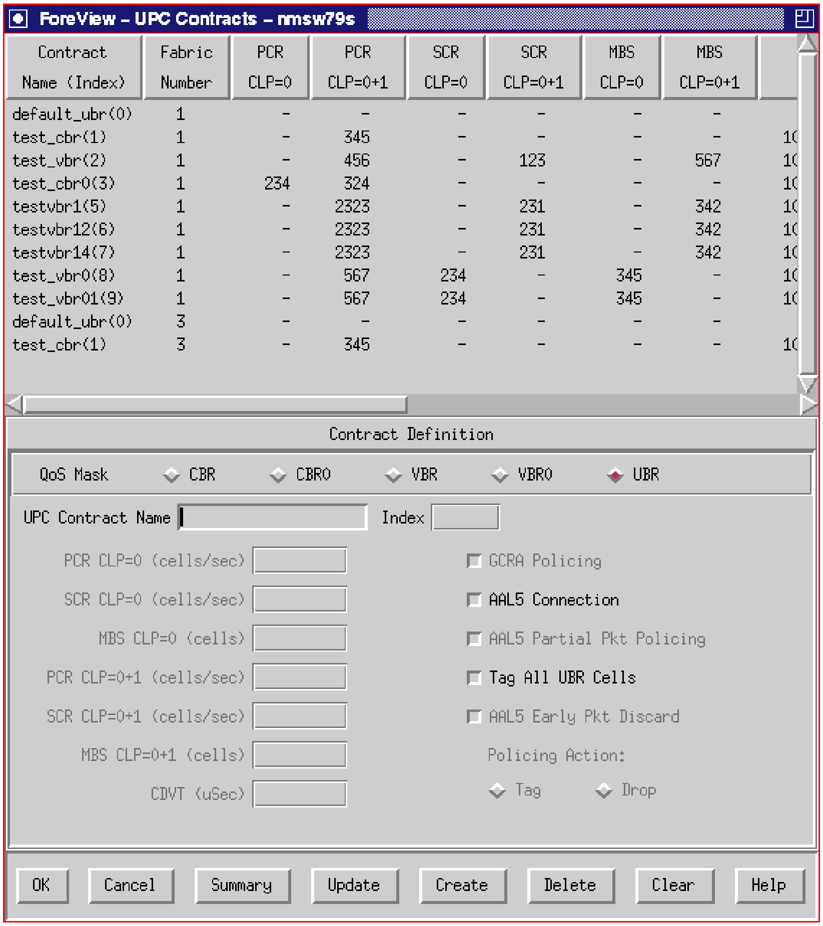
The UPC Contracts dialog is expanded when the **`Details`** button in the UPC dialog is clicked. The upper portion of the dialog displays detailed UPC contract information, including the contract name, various cell rates and the various traffic management options such as policing status. An example is shown below.

The **`Details`** dialog is a multi-column list box. The columns can be rearranged by clicking on the column headings, thus allowing you to reposition columns. To move a column towards the left, first click on the column that is to be moved, next click on any column to the left. The first column is moved to the left of the second column. To move a column towards the right, first click on the column that is to be moved, next click on any column to the right. The first column is moved to the right of the second column.

NOTE Any changes to the order of the columns are lost when the dialog is closed. Upon reopening the dialog, the order of the columns reverts back to the default order. A horizontal scroll bar is available to view parts of the list which are not immediate visible.

Clicking the **`Summary`** button closes the **`Details`** portion of the dialog, but does not close the main UPC Contracts dialog. Clicking the **`Update`** button refreshes the list of contracts and their details.

Changes to the main UPC Contracts dialog's list box are not automatically reflected in the **`Details`** dialog. The **`Details`** dialog must be explicitly updated by clicking the **`Update`** button to see any changes initiated from the main UPC Contracts dialog.



Contract Name (Index)	Fabric Number	PCR CLP=0	PCR CLP=0+1	SCR CLP=0	SCR CLP=0+1	MBS CLP=0	MBS CLP=0+1	
default_ubr(0)	1	-	-	-	-	-	-	
test_cbr(1)	1	-	345	-	-	-	-	10
test_vbr(2)	1	-	456	-	123	-	567	10
test_cbr0(3)	1	234	324	-	-	-	-	10
testvbr1(5)	1	-	2323	-	231	-	342	10
testvbr12(6)	1	-	2323	-	231	-	342	10
testvbr14(7)	1	-	2323	-	231	-	342	10
test_vbr0(8)	1	-	567	234	-	345	-	10
test_vbr01(9)	1	-	567	234	-	345	-	10
default_ubr(0)	3	-	-	-	-	-	-	
test_cbr(1)	3	-	345	-	-	-	-	10

Contract Definition

QoS Mask ◇ CBR ◇ CBR0 ◇ VBR ◇ VBR0 ◆ UBR

UPC Contract Name

Index

PCR CLP=0 (cells/sec)

SCR CLP=0 (cells/sec)

MBS CLP=0 (cells)

PCR CLP=0+1 (cells/sec)

SCR CLP=0+1 (cells/sec)

MBS CLP=0+1 (cells)

CDVT (uSec)

□ GCRA Policing

□ AAL5 Connection

□ AAL5 Partial Pkt Policing

□ Tag All UBR Cells

□ AAL5 Early Pkt Discard

Policing Action: ◇ Tag ◇ Drop

Figure 9.17 - UPC Contracts Dialog with Details

9.11 General Concepts of UPC Contracts

UPC contracts ensure that the connections that reserve bandwidth are not exceeding their reservations. FORE Systems' switches use a combination of "leaky bucket," or Generic Cell Rate Algorithm (GCRA) hardware in the switch fabric and user-configurable parameters in Virtual Path/Channel tool to perform these policing functions.

9.11.1 Setting the CLP Bit

First, it is important to understand the concept of tagging and dropping. Each ATM cell has a Cell Loss Priority (CLP) bit which indicates if the network can drop it under congested conditions. When the CLP bit is set to 0 (or CLP = 0), the cell will be assessed for compliance with traffic parameters. If the traffic parameters dictate that non-compliant cells should be "tagged", the CLP bit will be set to 1 (or CLP = 1), which means that upon experiencing congestion further in the network, these CLP = 1 cells will be dropped (because you cannot tag them again).

9.11.2 Leaky Bucket Algorithm

The next important concept is the leaky bucket algorithm. Leaky buckets are a mechanism by which cells entering the switch fabric are monitored for compliance with UPC traffic contracts that have been negotiated at connection set-up time. Before the leaky buckets are discussed, it is important to understand the parameters that are being measured by the buckets. They are as follows:

- Peak Cell Rate (PCR) - the maximum number of cells per second.
- Cell Delay Variation Tolerance (CDVT) - the tolerance for variation in the interarrival time of these cells, or the amount of jitter that can be accepted by the network.
- Sustainable Cell Rate (SCR) - the average rate of cell transmission for this connection, taking bursting into account.
- Maximum Burst Size (MBS) - the maximum amount of cells that can be transmitted at the PCR.

The leaky bucket algorithm is a timer which measures the cells entering the switch fabric against the parameters listed above. As a cell arrives, the timer assesses if the cell is on time, late, or early. If the cell is determined to be on time or late (within the traffic parameters specified), the cell is allowed to pass and no changes are made to its CLP bit. If the cell is early (which exceeds the specified parameters and would create congestion), the cell is either dropped or tagged (the CLP bit is set to 1), depending on the specified contract.

The first bucket in this analogy measures the PCR, or the rate at which the bucket drains. It also considers the CDVT, or the depth of the bucket. The second bucket measures the SCR, or the rate at which the bucket drains, and the MBS, or the depth of the second bucket.

9.11.3 UNI 3.x UPC Traffic Contract Parameters

The ATM Forum has defined different types of traffic contracts to be used in conjunction with these leaky buckets. The parameters that make up these types of contracts are defined as follows:

- pcr0 - measures PCR for cells with CLP = 0
- pcr01 - measures PCR for cells with CLP = 0 + cells with CLP = 1 (all cells)
- scr0 - measures SCR for cells with CLP = 0
- scr01 - measures SCR for cells with CLP = 0 + cells with CLP = 1 (all cells)
- mbs0 - measures MBS for cells with CLP = 0
- mbs01 - measures MBS for cells with CLP = 0 + cells with CLP = 1 (all cells)
- tag - sets CLP bit = 1 for non-compliant CLP = 0 cells

The specific combinations of these parameters that make up the ATM Forum contracts are defined as follows:

1. ubr
2. cbr <pcr01>
3. cbr0 <pcr0> <pcr01> [tag]
4. vbr <pcr01> <scr01> <mbs01>
5. vbr0 <pcr01> <scr0> <mbs0> [tag]

The **`ubr`** contract is for UBR traffic. Since this is best-effort traffic with no bandwidth guarantees provided, this type of traffic can not be policed against bandwidth parameters.

The **`cbr <pcr01>`** contract is for CBR traffic. It only uses the first leaky bucket to assess the PCR of the combination of CLP = 0 cells plus the CLP = 1 cells. All non-compliant cells are dropped.

The **`cbr0 <pcr0> <pcr01> [tag]`** contract is for CBR traffic. It uses the first leaky bucket to assess the PCR of the combination of CLP = 0 cells plus the CLP = 1 cells and to assess the group of CLP = 0 cells separately. All non-compliant cells in both groups are dropped if the tag option is not set. If the tag option is set, the non-compliant CLP = 0 cells in both groups are tagged and the non-compliant CLP = 1 cells are dropped.

The **vbr <pcr01> <scr01> <mbs01>** contract is for VBR traffic. It uses both leaky buckets simultaneously. The first bucket assesses the PCR of the combination of CLP = 0 cells plus the CLP = 1 cells and the second bucket assesses the SCR and MBS of this same combination. All non-compliant cells are dropped even if they comply with one bucket.

The **vbr0 <pcr01> <scr0> <mbs0> [tag]** contract is for VBR traffic. It uses both leaky buckets simultaneously, as well. The first bucket assesses the PCR of the combination of CLP = 0 cells plus the CLP = 1 cells, but the second bucket assesses the SCR and MBS of CLP = 0 cells only. All non-compliant cells are dropped even if they comply with one bucket, provided that the tag option is not set. If the tag option is set, the non-compliant CLP = 0 cells in all groups are tagged and the non-compliant CLP = 1 cells are dropped.

NOTE

Remember, when you create a UPC contract, it is not actually used until you assign it to a PVC, PVP, or the connectionless service of a SPANS signalling path.

CHAPTER 10 Tracking Network Usage

ForeView includes graphing and logging usage utilities which allow you to track network usage. These tools allow you to select a set of ATM switches, links, and hosts to be tracked.

NOTE

Users of *ForeView* running under SunNet Manager or WindowsNT use the default **`fvbltgr`** utility. Users of *ForeView* running under HP OpenView use OpenView's **`xnmgraph`** utility. The selection options are the same under all platforms.

The graph tools (**`fvgraph, fvgraphp, fvgraphc,`** and **`fvgraphh`**) show usage information for the network entities you select. For a selected link, switch, or host (or multiple selections), you can graph statistics for switch ports, paths, and channels independently.

The log tools (**`fvlog, fvlogp, fvlogc,`** and **`fvlogh`**) collect usage information and store it in log files which can be imported into databases or spreadsheets. For a selected link, switch, or host (or multiple selections), you can log information about switch ports, paths, and channels independently. You can also log host data.

Both tools are integrated into the *ForeView* menu within OpenView, SunNet Manager, and the Stand-alone Map. Also, both tools can be run outside of OpenView from the command line. Please refer to the man pages in Appendix A for more information on the command line usage of these tools.

10.1 Graphing Network Usage Overview

To use *ForeView* to graph network usage, simply select what you want to track in the **ATM Networks** submap or view, the **ATM Switch Connections** submap or view, the **Inter-switch Connections** submap or view, or a labeled link. Then, access the tool menus and select one of the four graphing menu items: switch ports, switch paths, switch channels, or hosts. This method works for graphing network usage for switches, links, and hosts in your network.

10.1.1 The Graph Tools

The following graphing options are available:

Graph / Switch Ports Starts the Graph Tool for selecting ports and parameters for selected switches or labeled links.

Graph / Switch Paths Starts the Graph Tool for selecting paths and parameters for selected switches or labeled links.

Graph / Switch Channels Starts the Graph Tool for selecting channels and parameters for selected switches or labeled links.

Graph / Hosts Starts the Graph Tool for selecting parameters to graph for selected hosts, labeled links, or switches.

For any graph menu item selected, a dialog appears asking you to specify parameters that you would like to graph. The graph collection interval defaults to 15 seconds. To change the default, change the **Collection Interval** in the selection dialog.

For ports, select **Cells Tx (Transmitted), Cells Rx (Received),** or **Additional Parameters**.

For paths and channels, select **Cells Rx (Received),** or **Rejected (Cells Rejected)**. Paths also have **Additional Parameters**.

For hosts, select **Cells Tx (Transmitted), Cells Rx (Received),** or **Additional Parameters**.

When you are done specifying graph parameters, click on **Apply** to start graphing the items you selected.

If you want to cancel without starting up a graph, press **Cancel**.

10.1.2 Selection Options

When selecting a switch for graphing, you are able to choose from all the enabled ports on that switch (or switches), including the control port. The control port is an internal port which carries traffic to and from the control processor. The type of traffic generated and received by a switch includes network management (SNMP) traffic.

To graph usage by a host, select the host(s) that you wish to track. Tracking usage by specific hosts in your network allows you to track a single user or user group in your network. For example, to track usage for the marketing department, select the hosts in marketing, choose **`Graph/Hosts..., select the parameters, and launch a graph`**.

10.1.2.1 Graphing Switch Options Summary

In general, when graphing switch options (ports, paths, channels) using the Graph Tools:

- Graph switch options from switches selected from the **ATM Networks** submap or view, the **ATM Switch Connections** submap or view, the **Inter-switch Connections** submap or view, and the **Stand-alone** map.
- Graph switch options from links selected in the **ATM Switch Connections** submap and the **Inter-switch Connections** submap.

10.1.2.2 Graphing Host Options Summary

In general, when graphing host statistics using the Graph Tools:

- Select hosts from the **ATM Switch Connections** submap or view, either by selecting a host icon or by selecting a host-to-switch link (HP OpenView).

NOTE

In a host-to-switch link, the **`Graph/Hosts`** option always graphs the host statistics.

- Select hosts from the **Stand-alone** map by selecting a host icon.
- When you select a host icon from the map or view, switch graph options (ports, paths, channels) are disabled, and only the host graph option is available.
- Selecting a link between a host and a switch allows you to graph for the host, and also allows you to graph the switch parameters (ports, paths, channels).

NOTE

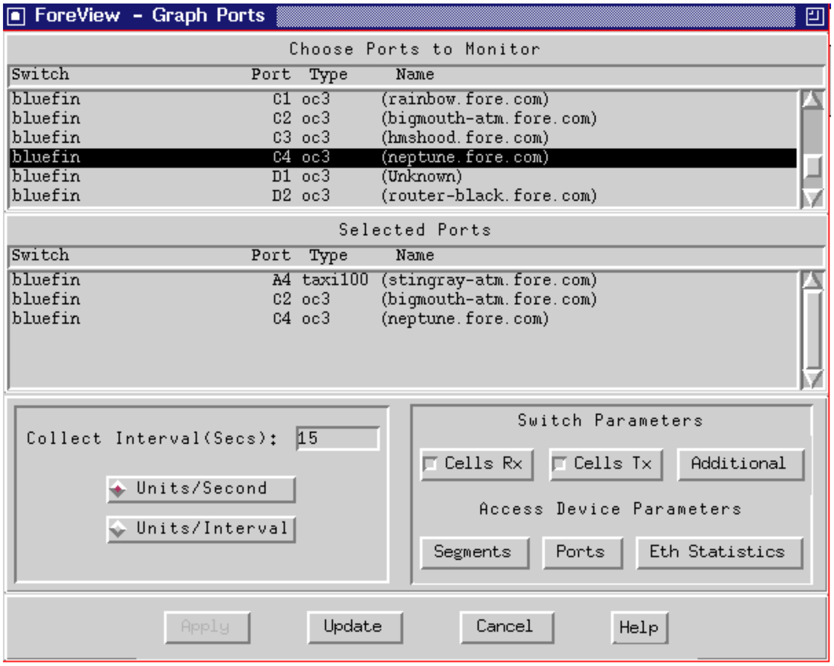
When a host is connected to a switch and that host is not transmitting IP traffic the host is identified as *switch port-**bnp*** where ***b*** is the board, ***n*** is the network module, and ***p*** is the port on the switch to which the host is attached. If a host is not transmitting IP, **`Graph/Host`** will not work because the graph tool relies on the host to reply to the SNMP agent, which runs on top of IP.

Table 10.1 - Graph Selection Summary

	Parameters	Additional Parameters
Ports	Cells Received Cells Transmitted	Ports Errors Shared Memory Statistics Netmod Statistics (Sonet, DS3, DS1, J2, E3, E1, TP-25) Access Device Parameters
Paths	Cells Received Cells Rejected	SPANS Signalling UNI 3.0 Signalling
Channels	Cells Received Cells Rejected	None
Hosts	Cells Received Cells Transmitted	Physical Layer Errors ATM Layer Statistics AAL Statistics Sonet Statistics Access Device Parameters

10.1.3 Graphing Example

When you select **`Graph/Switch Ports`**, a pop-up dialog allows you to select ports and parameters for graphing, as illustrated below.



ForeView - Graph Ports

Choose Ports to Monitor

```
Switch                  Port  Type    Name
bluefin                   C1  oc3    (rainbow.fore.com)
bluefin                   C2  oc3    (bigmouth-atm.fore.com)
bluefin                   C3  oc3    (hmshood.fore.com)
bluefin                   C4  oc3    (neptune.fore.com)
bluefin                   D1  oc3    (Unknown)
bluefin                   D2  oc3    (router-black.fore.com)
```

Selected Ports

```
Switch                  Port  Type    Name
bluefin                   A4  taxi100 (stingray-atm.fore.com)
bluefin                   C2  oc3    (bigmouth-atm.fore.com)
bluefin                   C4  oc3    (neptune.fore.com)
```

Collect Interval(Secs): 15

◆ Units/Second

◇ Units/Interval

Switch Parameters

□ Cells Rx □ Cells Tx Additional

Access Device Parameters

Segments Ports Eth Statistics

Apply Update Cancel Help

Items selected here...

...are displayed here.

Collection Interval defaults to 15 secs.

Figure 10.1 - Graph Switch Ports Selection Dialog

A port can be removed from the Selected Ports dialog simply by clicking on the port with the left mouse button. Also, you can select additional statistics to graph by clicking on the **`Additional Parameters`** button.

When you select **`Additional Parameters`**, a pop-up dialog allows you to select other statistics for graphing based on port type, as illustrated below.

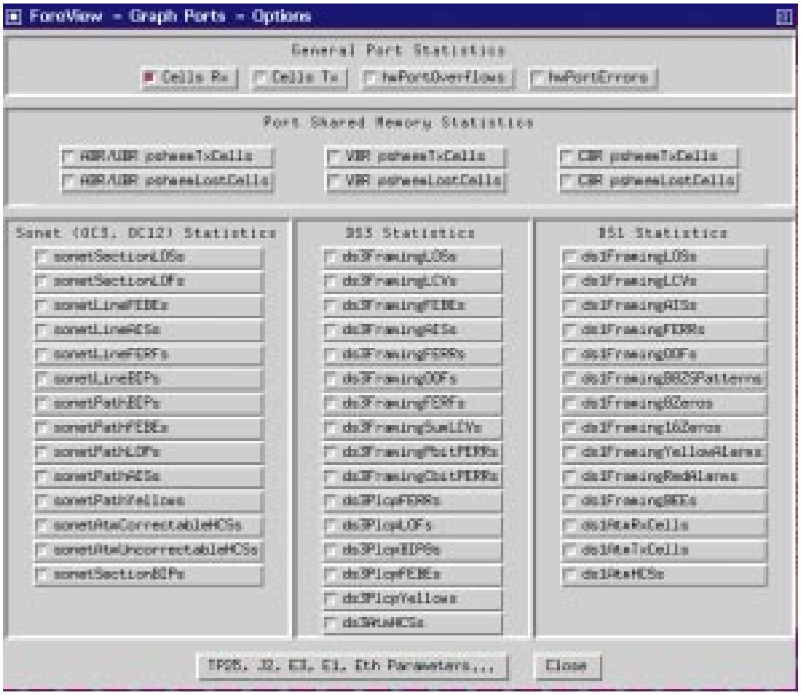


Figure 10.2 - Additional Parameters Dialog for Port Graphing

NOTE

Selections from **`Additional Parameters`** take effect immediately. The pop-up dialog does not need to be closed to apply the parameters for graphing.

After all parameters have been selected, launch the switch port graph by clicking on the **`Apply`** button from the **`Graph/Switch Ports`** selection dialog. A graph of the ports selected in Figure 10.1 might look the following:

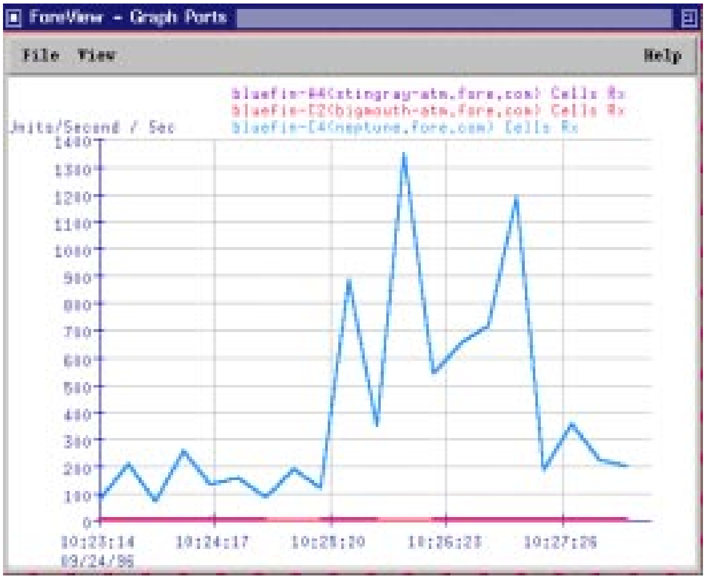


Figure 10.3 - Typical Switch Port Graph

NOTE

Switches can also act as hosts. If you graph host statistics from a switch, what you actually graph is the control port traffic for that switch.

NOTE

Non-IP hosts also show up in the map without a hostname label whereas IP hosts have a hostname label on the icon. If a host is not transmitting IP, **`Graph/Host`** will not work because the graph tool relies on the host to reply to the SNMP agent, which runs on top of IP.

10.2 Logging Network Usage Overview

Graphing network usage is a desirable capability to track utilization in real-time. Often, however, you may want to collect usage information in the background for later analysis. Monthly network usage reports and billing reports are examples of when logging network usage information is useful. *ForeView* provides a mechanism to log ATM network usage.

Logging network usage is very similar to graphing network usage. In general, anything that can be graphed also can be logged. Select the items in your ATM network that you wish to track: switches, links, and hosts. Then select one of the four log options. *ForeView* opens a dialog (similar to the graphing dialogs) that lets you customize your log in terms of parameters, collection intervals, and log names.

10.2.1 The Log Tools

The following options for logging are available from *ForeView*:

Log / Switch Ports Starts the Log Tool for selecting ports, collection intervals, and parameters for selected switches or labeled links.

Log / Switch Paths Starts the Log Tool for selecting paths, collection intervals, and parameters for selected switches or labeled links.

Log / Switch Channels Starts the Log Tool for selecting channels, collection intervals, and parameters for selected switches or labeled links.

Log / Hosts Starts the Log Tool for selecting parameters to log for selected hosts, labeled links, or switches.

10.2.2 Selection Options

When selecting a switch for logging, you are able to choose from all the enabled ports on that switch (or switches), including the control port. The control port is an internal port which carries traffic to and from the control processor. The type of traffic generated and received by a switch includes network management (SNMP) traffic.

To log usage by a host, select the host(s) that you wish to track. Tracking usage by specific hosts in your network allows you to track a single user or user group in your network. For example, to track usage for the marketing department, select the hosts in marketing, choose **`Log/Hosts..., select the parameters, and start the log process`**.

10.2.2.1 Logging Switch Options Summary

In general, when logging switch options (ports, paths, channels) using the Log Tools:

- Log switch options from switches selected from the **ATM Networks** submap or view, the **ATM Switch Connections** submap or view, the **Inter-switch Connections** submap or view, and the **Stand-alone** map.
- Log switch options from links selected in the **ATM Switch Connections** submap and the **Inter-switch Connections** submap.

10.2.2.2 Logging Host Options Summary

In general, when logging host statistics using the Log Tools:

- Select hosts from the **ATM Switch Connections** submap or view, either by selecting a host icon or by selecting a host-to-switch link (HP OpenView).

NOTE

In a host-to-switch link, the **`Log/Hosts`** option always graphs the host statistics.

- Select hosts from the **Stand-alone** map by selecting a host icon.
- When you select a host icon from the map or view, switch log options (ports, paths, channels) are disabled, and only the host log option is available.
- Selecting a link between a host and a switch allows you to log for the host, and also allows you to log the switch parameters (ports, paths, channels).

NOTE

Switches can also act as hosts. If you log host statistics from a switch, what you actually log is the control port traffic for that switch.

NOTE

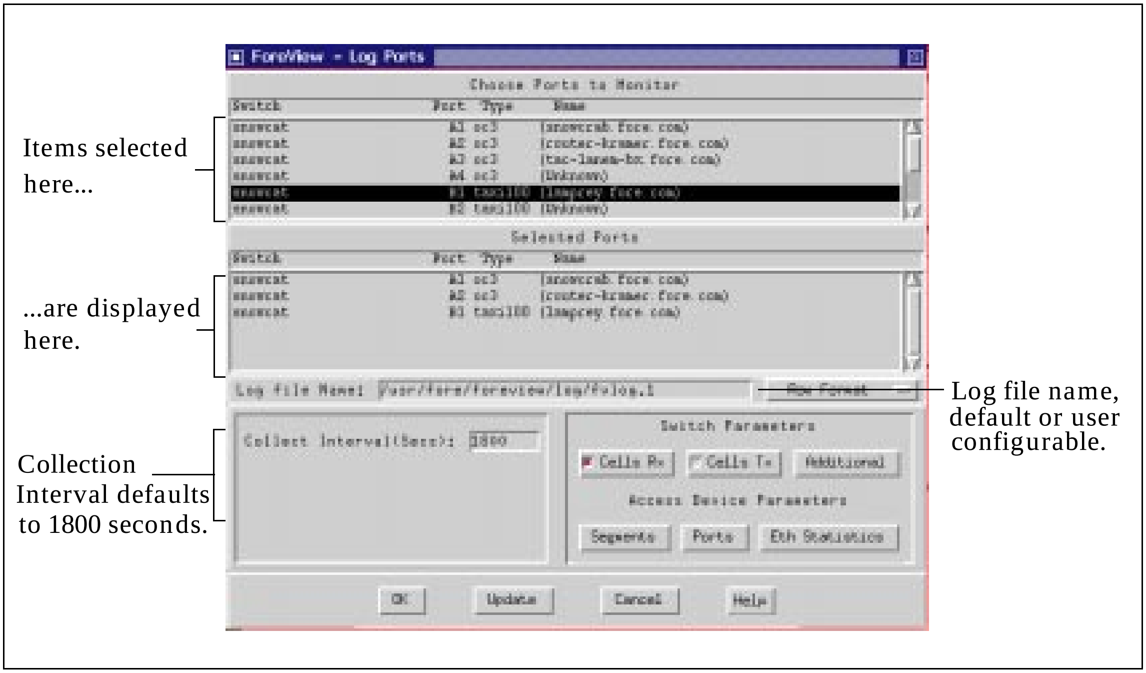
Non-IP hosts also show up in the map without a hostname label whereas IP hosts have a hostname label on the icon. If a host is not transmitting IP, **`Log/Host`** does not work because the log tool relies on the host to reply to the SNMP agent, which runs on top of IP.

Table 10.2 - Log Selection Summary

	Parameters	Additional Parameters
Ports	Cells Received Cells Transmitted	Ports Errors Shared Memory Statistics Netmod Statistics (Sonet, DS3, DS1, J2, E3, E1, TP-25) Access Device Parameters
Paths	Cells Received Cells Rejected	SPANS Signalling UNI 3.0 Signalling
Channels	Cells Received Cells Rejected	None
Hosts	Cells Received Cells Transmitted	Physical Layer Errors ATM Layer Statistics AAL Statistics Sonet Statistics Access Device Parameters

10.2.3 Logging Example

When you select **`Log/Switch Ports`**, a pop-up dialog allows you to select ports and parameters for graphing, as illustrated below.



ForeView - Log Ports

Choose Ports to Monitor

Switch	Port	Type	Name
snowcat	A1	oc3	(snowcrab.fore.com)
snowcat	A2	oc3	(coutec-kramer.fore.com)
snowcat	A3	oc3	(tac-lanem-bx.fore.com)
snowcat	A4	oc3	(Unknown)
snowcat	B1	taxi100	(lamprey.fore.com)
snowcat	B2	taxi100	(Unknown)

Selected Ports

Switch	Port	Type	Name
snowcat	A1	oc3	(snowcrab.fore.com)
snowcat	A2	oc3	(coutec-kramer.fore.com)
snowcat	B1	taxi100	(lamprey.fore.com)

Log file Name: /usr/fore/foreview/log/fvlog.1 Raw Format

Collect Interval(Secs): 1800

Items selected here...

...are displayed here.

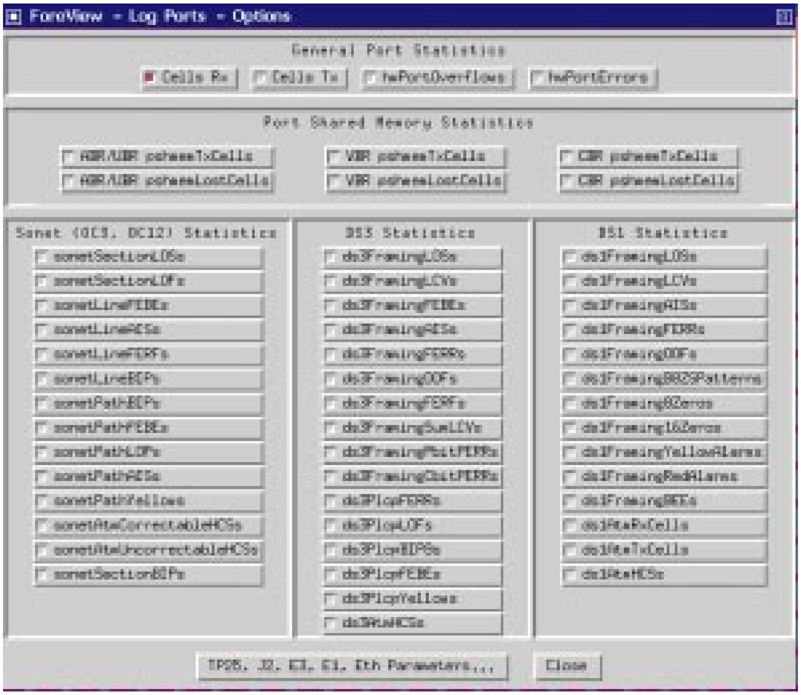
Collection Interval defaults to 1800 seconds.

Log file name, default or user configurable.

Figure 10.4 - Log Switch Ports Selection Dialog

A host can be removed from the Selected Hosts dialog simply by clicking on the host with the left mouse button. Also, you can select additional statistics to log by clicking on the **`Additional Parameters`** button.

When you select **`Additional Parameters`**, a pop-up dialog allows you to select other statistics for logging based on host adapter type, as illustrated below.


ForeView - Log Ports - Options
TP25, J2, E3, E1, Eth Parameters...
Close

General Port Statistics

☑ Cells Rx
□ Cells Tx
□ hwPortOverflows
□ hwPortErrors

Port Shared Memory Statistics

□ ABR/UBR pshmemTxCells
□ ABR/UBR pshmemLostCells
□ VBR pshmemTxCells
□ VBR pshmemLostCells
□ CBR pshmemTxCells
□ CBR pshmemLostCells

Sonet (OC3, OC12) Statistics

□ sonetSectionLOSs
□ sonetSectionLOFs
□ sonetLineFEBEs
□ sonetLineAISs
□ sonetLineFERFs
□ sonetLineBIPs
□ sonetPathBIPs
□ sonetPathFEBEs
□ sonetPathLOPs
□ sonetPathAISs
□ sonetPathYellows
□ sonetAtmCorrectableHCSs
□ sonetAtmUncorrectableHCSs
□ sonetSectionBIPs

DS3 Statistics

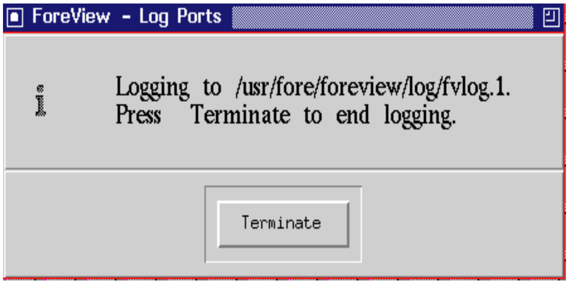
□ ds3FramingLOSs
□ ds3FramingLCVs
□ ds3FramingFEBEs
□ ds3FramingAISs
□ ds3FramingFERRs
□ ds3FramingOOFs
□ ds3FramingFERFs
□ ds3FramingSumLCVs
□ ds3FramingPbitPERRs
□ ds3FramingCbitPERRs
□ ds3PlcpFERRs
□ ds3PlcpLOFs
□ ds3PlcpBIP8s
□ ds3PlcpFEBEs
□ ds3PlcpYellows
□ ds3AtmHCSs

DS1 Statistics

□ ds1FramingLOSs
□ ds1FramingLCVs
□ ds1FramingAISs
□ ds1FramingFERRs
□ ds1FramingOOFs
□ ds1FramingB8ZSPatterns
□ ds1Framing8Zeros
□ ds1Framing16Zeros
□ ds1FramingYellowAlarms
□ ds1FramingRedAlarms
□ ds1FramingBEEs
□ ds1AtmRxCells
□ ds1AtmTxCells
□ ds1AtmHCSs

Figure 10.5 - Log Switch Ports Additional Parameters

Once logging has begun, a log message dialog appears, as shown in Figure 10.6. This dialog indicates that a logging process is running in the background. To terminate logging, select the **`Terminate`** button on the log message dialog. Normally, once you begin logging, you should minimize this box so it is out of the way (but always present to indicate that logging is happening).



Logging to /usr/fore/foreview/log/fvlog.1.
Press Terminate to end logging.

Figure 10.6 - Log Message Dialog

The output of logging is a comma-delimited ASCII file. The format of the output log file for switch-based logging is as follows:

```
#date, time, switch port(hostname) variable, value
```

The format of the output log file for host adapter-based logging is as follows:

```
#date, time, host variable, value
```

The **date** and **time** indicate the time that data was collected. The **switch** is the switch to which the logged entity is attached. The **port** is the port number to which the entity is attached. The **hostname** is the IP hostname of the entity being logged. This is blank if the entity does not speak IP. The **variable** is the SNMP variable, or statistic, that is being monitored. Finally, the **value** is the number of 53-byte ATM cells for that variable transmitted and received by that entity over the data collection interval.

Here are two examples from log files. The first example shows three different ports on the switch angler. Each one is logging the Cells Received parameter on path 0.

```
          #date,time,switch-port(host) variable,value
          08/25/94,00:08:40,angler-B1(dnsmim-atm)/0 Cells Rx,76082
08/25/94,00:08:40,angler-A2(bluewhale-atm)/0 Cells Rx,59207
          08/25/94,00:08:40,angler-A4(humpback-atm)/0 Cells Rx,28493
```

The second example tracks the host-adapter MIB on 2 different hosts (the host netmgtsw2 happens to be the control port on a switch). The parameters logged from each host adapter consist of: Received Cells, Transmitted Cells, aal5CellDiscards, aal4PayloadCRCErrors, aal4SARProtocolErrors and aal4CSProtocolErrors.

```
#date,time,host variable,value
08/25/94,15:36:07,cadlina-atm Received Cells ,99
08/25/94,15:36:07,cadlina-atm Transmitted Cells,58
08/25/94,15:36:07,cadlina-atm aal5CellDiscards,0
08/25/94,15:36:07,cadlina-atm aal4PayloadCRCErrors,0
08/25/94,15:36:07,cadlina-atm aal4SARProtocolErrors,0
08/25/94,15:36:07,cadlina-atm aal4CSProtocolErrors,0
08/25/94,15:36:07,netmgtsw2 Received Cells ,498
08/25/94,15:36:07,netmgtsw2 Transmitted Cells,619
08/25/94,15:36:07,netmgtsw2 aal5CellDiscards,0
08/25/94,15:36:07,netmgtsw2 aal4PayloadCRCErrors,0
08/25/94,15:36:07,netmgtsw2 aal4SARProtocolErrors,0
08/25/94,15:36:07,netmgtsw2 aal4CSProtocolErrors,0
```

Most standard databases and spreadsheets import comma-delimited ASCII files. The logging mechanism built into *ForeView* is a powerful way to collect usage and accounting information from your *ForeRunner* ATM network.

10.3 Billing for Network Usage

ForeView provides a background logging mechanism that allows you to track network utilization over long periods of time. You can log utilization information for hosts, links, and switches in your network. This information can be imported into spreadsheets and databases. It can be used to understand long-term utilization trends in your network, to track billing information from a public ATM carrier, or even to allocate the cost of maintaining a network among the users of that network.

Suppose you wanted to bill users based on network utilization. Suppose the operating cost of installing and running the network is $10,000 per month and you want to bill out 50% of this cost on a flat rate per user and bill the other 50% based on actual network usage. Let’s see how you can use *ForeView*’s logging mechanism to bill based on usage.

To start collecting usage information for all users in the network:

1. Select all ATM switches in the network.
2. Select the hosts that you want to include.
3. Choose **`Log / Switch Ports...`** to start logging by port for all switches and hosts in your network.

You may either time the start-up of logging so that it coincides with your billing interval or you may hand-edit the log file so that it contains data only for the billing interval. Below is a clip of a log file that covers a month of usage information for all hosts in an ATM network.

```
#date,time,switch-port(host) variable,value
08/01/94,00:26:14,bluefin.fore.com-C1(stein-atm)Cells Tx,152011
08/01/94,00:26:14,bluefin.fore.com-A1(angler) Cells Tx,94165
08/01/94,00:26:14,bluefin.fore.com-D4(catfish-atm) Cells Tx,16957
08/01/94,00:26:14,bluefin.fore.com-D3(crayfish) Cells Tx,18533
08/01/94,00:26:14,bluefin.fore.com-B2(turtle) Cells Tx,17427
.
.
.
08/31/94,23:56:14,bluefin.fore.com-C1(stein-atm)Cells Tx,151394
08/31/94,23:56:14,bluefin.fore.com-A1(angler) Cells Tx,159664
08/31/94,23:56:14,bluefin.fore.com-D4(catfish-atm) Cells Tx,17468
08/31/94,23:56:14,bluefin.fore.com-D3(crayfish) Cells Tx,19051
08/31/94,23:56:14,bluefin.fore.com-B2(turtle) Cells Tx,17956
```

This file can be easily processed by spreadsheet and database programs. In this example, awk is used to glean billing information from the log file. There are 4 columns of comma-delimited data.

```
#date,time,switch-port(host) variable,value
```

We need to tally each host's contribution and to compute the percentage contribution of that host to the total traffic sent. To do this, we only look at the host field (*in awk* - ***$3***) and the transmit counts (*in awk* - ***$4***). Because this data is gathered from the switch perspective, this represents traffic sent from the switch to the host.

Here is an awk program to calculate a bill for each host in which half of the bill is a flat rate of $1000 per user and the other half is that hosts's allocation based on its usage of the network.

```
BEGIN {
          FS=","
}

!/^#/  {  # for lines that do not begin with a comment...
          host[ $3 ] += $4
          total += $4
}

END  {
  for ( name in host ) {
                     printf "$%7.2f  (%d)  %s\n", \
                      host[ name ] * 5000 / total + 1000,\
                                host[ name ], \
                                name
                   }
}
```

Running this program, **awk -f bill.awk fvlog.1** yields:

```
awk -f bill.awk fvlog.5
$5049.94  (871858171)  bluefin.fore.com-C1(stein-atm) Cells Tx
$1912.26  (196388742)  bluefin.fore.com-A1(angler) Cells Tx
$1021.24  (4571726)  bluefin.fore.com-D4(catfish-atm) Cells Tx
$1011.59  (2496038)  bluefin.fore.com-D3(crayfish) Cells Tx
$1004.97  (1070606)  bluefin.fore.com-B2(turtle) Cells Tx
```

Notice that in this network, most of the users pay close to the flat rate. This is just one example of how to use network usage information to manage your network. Importing the information into a spreadsheet to create a report on network usage is another example. Tracking a link into a public network to confirm billing information from a public service provider is another example.

10.4 Graphing and Logging from the Command-line

For convenience, *ForeView*'s Graphing and Logging can be run from the command-line of your operating system. There are four variations of graphing/logging:

- fvgraphh/fvlogh – graph/log network usage and error statistics on hosts in a ForeRunner ATM network
- fvgraph/fvlog – graph/log network usage and error statistics on switch ports in a ForeRunner ATM network
- fvgraphp/fvlogp – graph/log network usage on switch paths
- fvgraphc/fvlogc – graph/log network usage on switch channels

The following explains the command-line syntax:

fvgraphh/fvlogh *[-cr community_read_name] [-cw community_write_name] [-interval collection_interval] host [host]...*

fvgraph/fvlog *[-cr community_read_name] [-cw community_write_name] [- interval collection_interval]* -ABR|-Abr|-abr -VBR|-Vbr|-vbr -CBR|-Cbr|-cbr -DS1|-Ds1|-ds1 -DS3|-Ds3|ds3 -OC3|-Oc3|-oc3 -OC12|-Oc12|-oc12 -E1|-e1 -E3|-e3 -J2|-j2 -TP25|-Tp25|-tp25 -ETH|-eth *switch [switch]...*

fvgraphp/fvlogp *[-cr community_read_name] [-cw community_write_name] [-interval collection_interval] switch [switch]...*

fvgraphc/fvlogc *[-cr community_read_name] [-cw community_write_name] [-interval collection_interval] switch [switch]...*

WHERE *host* is the IP hostname of a host, switch, PowerHub in a ForeRunner ATM network. *switch* is the IP hostname or ATM address of a switch or powerhub in a ForeRunner ATM network or a link identifier in the format <switch_hostname>:<port_identifier>. *port_identifier* is the nomenclature used by all the ForeView and ForeRunner tools to identify ports. Example: For the first port in network module "C" in an ASX-200, the port identifier is C1.

The following are line options for graphing and logging:

–ABR|-Abr|-abr
preselect the related ABR/UBR port shared memory statistic options

–VBR|-Vbr|-vbr
preselect the related VBR port shared memory statistic options

–CBR|-Cbr|-cbr
preselect the related CBR port shared memory statistic options

–DS1|-Ds1|-ds1
preselect the related DS1 statistic options

–DS3 | -Ds3 | -ds3
preselect the related DS3 statistic options

–E1 | -e1
preselect the related E1 statisticoptions

–E3 | -e3
preselect the related E3 statisticoptions

–OC3 | -Oc3 | -oc3
preselect the related OC1 statistic options

–OC12 | -Oc12 | -oc12
preselect the related OC12 statistic options

–J2 | -j2
preselect the related J2 statistic options

–TP25 | -Tp25 | -tp25
preselect the related TP25 statistic options

–ETH | -Eth | -eth
preselect the related Ethernet statistic options openview / atmdb / atmmon.db

–interval*collection_interval*
specify the collection interval in the unit of seconds.

CHAPTER 11 Channel and Path Tracing

In a typical ATM network there are many channels which carry data throughout a network. *ForeView* provides tools to help you understand the channels in *ForeRunner* ATM networks. The Virtual Channel/Path tool allows for PVC and Smart PVC (SPVC) configuration, and for browsing of virtual circuits. The channel grapher provides both channel browsing and graphing of channel usage.

ForeView's Channel/Path Tracer allows the tracing of channels from end-to-end in the network. These channel traces may be viewed in a tabular or graph format. Tabular traces show hop-by-hop the route that a virtual circuit takes through your ATM network. Graphs of channel traces show statistics from each hop that a channel takes through a network.

11.1 Uses for the Channel/Path Tracer

The Channel/Path Tracer can be used for several purposes including:

1. Isolation of hosts consuming the most bandwidth in a network.
2. Studies of node communication destinations.
3. Examinations of cell throughput, droppage, and rejections at each hop a channel makes as it traverses a network.

For example, one link in a network may be running at close to capacity. To isolate why that particular link is running at high capacity, *ForeView*'s channel grapher allows a detailed examination of utilization per channel on that link. If one or two channels are consuming most of the bandwidth on that link, *ForeView*'s Channel/Path Tracer can be invoked to determine the source of the traffic on the channel and which node is receiving the traffic.

To see which nodes a host in a network is communicating with, channels can be traced on the link between that host and its switch. This trace shows the destination of each channel originating from that host. If there is a performance problem between two hosts in the network, the Channel/Path Tracer can examine cell flows from end-to-end on the channel between those hosts. The Channel/Path Tracer's graphing facility allows tracking of cell flows and rejects at each hop that a channel makes through the network, allowing rapid isolation of problems on that channel as it traverses the network.

11.2 Tracing Channels and Paths in a Network

To trace a channel in a network, perform the following procedure:

1. Select the link or switch in the map which contains the channel to be traced.
2. Choose a channel on the link from the list of channels which appears.
3. Click on the **`Trace Channel/Path`** button.

11.2.1 Selecting Links and Switches for Tracing

Channels may be traced on a link or on a switch. To trace channels on a link, selection choices include inter-switch links or switch-to-host links in the network map.

To trace connections made by a particular host in a network:

1. Go to the switch connections map of the switch to which that host is connected.
2. Select the link between the host and the switch and invoke the Channel/Path Tracer.

To trace a channel on an inter-switch link:

1. Find the pair of switches in the ATM networks maps, and double-click on the meta link between the two switches.
2. Choose the link you wish to trace channels on and invoke the Channel/Path Tracer.

To trace channels on more than one link on a switch in your network:

1. Select that switch in the network map.
2. Invoke the Channel/Path Tracer. The Channel/Path Tracer will show channels on all of that switch’s links and allow tracing of any link.

The Channel/Path Tracer may also be launched after selecting any combination of links and switches in the map. To select more than one item in the map, hold down the **`ctrl`** key and select additional items with mouse clicks. The Channel/Path Tracer then shows all selected channels and links, allowing tracing any of these channels.

11.2.2 Tabular Traces

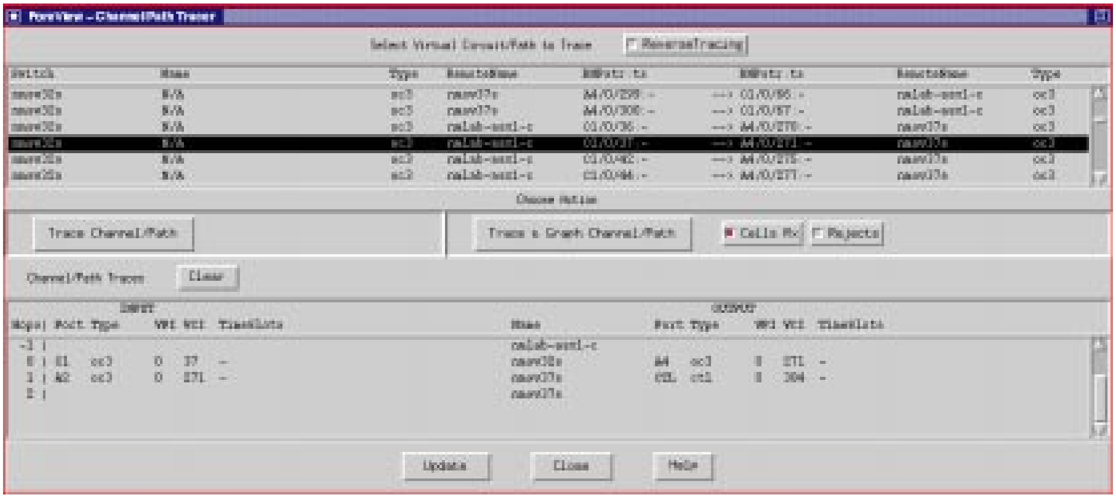
The Channel/Path Tracer displays channels in the top list box. For each channel, the following information is shown:

- The switch name and type of link
- The remote name BNP string (port/VP/VC/timeslot)
- The switch BNP string (port/VP/VC/timeslot)
- The name and type of link of the immediately attached switch or host

To trace a channel, simply select the channel in the upper list box and press the **`Trace Channel`** button. While the trace is underway, an hourglass is displayed. When the trace is completed, results appear in the list box in the bottom half of the screen. Previous results can be seen by scrolling the output list box. The **`Clear`** button will remove all entries from the output list box. The **`Update`** button will scan the original parameters and display all of the channels that were found using the selection parameters.

The following information is displayed:

- Each line of the trace shows a single hop on the channel's route from the channel's source to its destination.
- The left-hand column shows the number of hops to or from the trace point. Negative numbers indicate hops towards the source and positive numbers indicate hops towards the destination.
- The first line of the trace is the source of the channel.
- The last line of the trace is the destination of the channel.
- Each line in between shows a switch hop as the channel travels from its source to its destination.
- Each switch hop contains:
  - Hop count
  - Input port and type
  - Input VPI
  - Input VCI
  - Input Timeslot (for CES network modules)
  - Switch name
  - Output port and type
  - Output VPI
  - Output VCI
  - Output Timeslot (for CES network modules)



```
Switch     Name    Type  RemoteName      IfPort: ts        IfPort: ts    RemoteName      Type
nmsw32s    N/A     oc3   nmsw37s         A4/0/298:-   -->  C1/0/86:-     nmlab-asx1-c    oc3
nmsw32s    N/A     oc3   nmsw37s         A4/0/308:-   -->  C1/0/87:-     nmlab-asx1-c    oc3
nmsw32s    N/A     oc3   nmlab-asx1-c    C1/0/36:-    -->  A4/0/270:-    nmsw37s         oc3
nmsw32s    N/A     oc3   nmlab-asx1-c    C1/0/37:-    -->  A4/0/271:-    nmsw37s         oc3
nmsw32s    N/A     oc3   nmlab-asx1-c    C1/0/42:-    -->  A4/0/275:-    nmsw37s         oc3
nmsw32s    N/A     oc3   nmlab-asx1-c    C1/0/44:-    -->  A4/0/277:-    nmsw37s         oc3
```

```
              INPUT                                                OUTPUT
Hops| Port Type     VPI VCI  TimeSlots              Name           Port Type     VPI VCI  TimeSlots
 -1 |                                                nmlab-asx1-c
  0 | C1   oc3      0   37   -                       nmsw32s        A4   oc3      0   271  -
  1 | A2   oc3      0   271  -                       nmsw37s        CTL  ctl      0   304  -
  2 |                                                nmsw37s
```

Figure 11.1 - Tabular Trace

Figure 11.1 shows a tabular trace. Both the selection in the top list box and the line with a hop count of **`0`** in the bottom list box show that the trace was executed on channel **`0/37`** on port **`C1`** of switch **`nmsw32s`**. This channel starts at **`nmlab-asx1-c`** which is sending traffic on VPI/VCI **`0/37`**. It enters switch **`nmsw32s`** on port **`C1`** VPI/VCI **`0/37`** and gets remapped to VPI/VCI **`0/271`** as it exits on port **`A4`**. It then enters port **`A2`** VPI/VCI **`0/271`** on switch **`nmsw37s`** (exit VPI/VCI must match entry VPI/VCI on the next switch). On **`nmsw37s`** it is remapped to the control port on VPI/VCI **`0/304`**.

11.2.3 Graphing Traces

The operation of graphing channel/path traces is similar to making tabular traces. Selections are made in the map as follows:

1. Pull up the Channel/Path Tracer, and select a channel/path to trace.
2. Select which parameters are to be graphed. These parameters include cells and/or rejects.
3. Select the **`Trace & Graph Channel/Path`** button. When selected, channels/paths will be traced out to the end points as seen in the tabular trace. In addition to displaying the route through the network in tabular form, a graph dialog appears which shows selected statistics at each hop the channel/path makes from end-to-end.

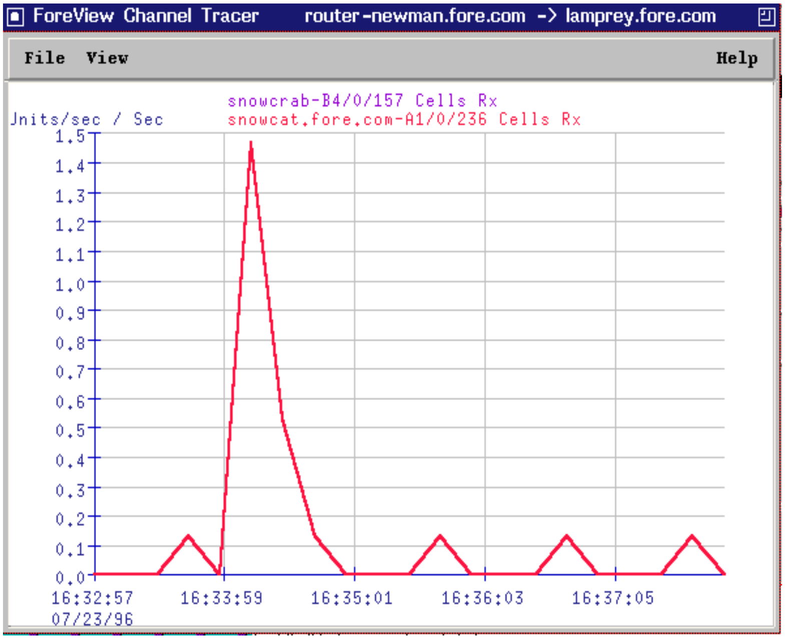


Figure 11.2 - Channel Trace Graph

When graphing both cells and rejects, ideally a graph should show a set of lines corresponding to cells at each hop where each of the **`Cells`** lines track the exact same pattern. Slight differences in SNMP data retrieval times from the different hop points can cause minor variations (<10%) in cell counts at each hop. Two or more distinct patterns in the **`Cells`** lines indicates cell loss, or droppage at a hop in your network, as shown in Figure 11.3.

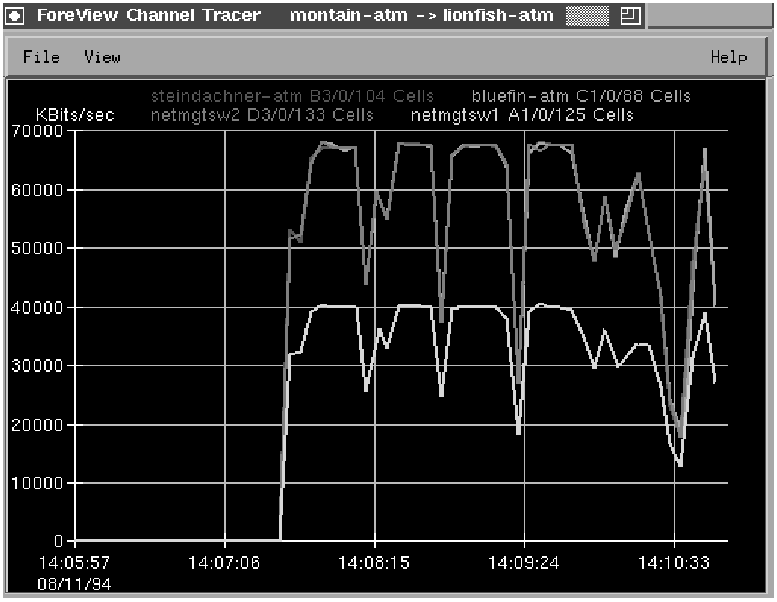


Figure 11.3 - Cell Loss

The hop which is losing cells can be determined by looking for a **`Cells`** line tracking noticeably lower than others. This lower tracking indicates other hops are seeing higher cells counts and that the droppage is occurring between the point seeing higher counts and the point seeing lower counts.

Cell loss can occur for a several reasons. Most likely, cell loss may occur due to overutilization. To check this, look at the graph of utilization on the link where cell loss is occurring to see if that link is operating near capacity.

Also check the **`Queue Overflows`** counter in the **`Port Status`** screen within the Front Panel. This counter should be zero when cells are not being dropped. While the **`Port Status`** text displays accurately reflect network status, many problems (especially intermittent ones) may be more easily diagnosed by looking at graphic trends.

Channel and Path Tracing

For example, Figure 11.3 shows how a framing loss occurs at a steady rate with occasional jumps. Such trends are difficult to determine from text. Another method of checking for cell loss is with a graph like Figure 11.4. Using the **ForeView - Graph -Switch Port** command stream, users can select from a number of graphing options common to DS-3, E-3, or OC-3c ports. Users may also graph parameters specific to DS-3, E-3, or OC-3c ports.

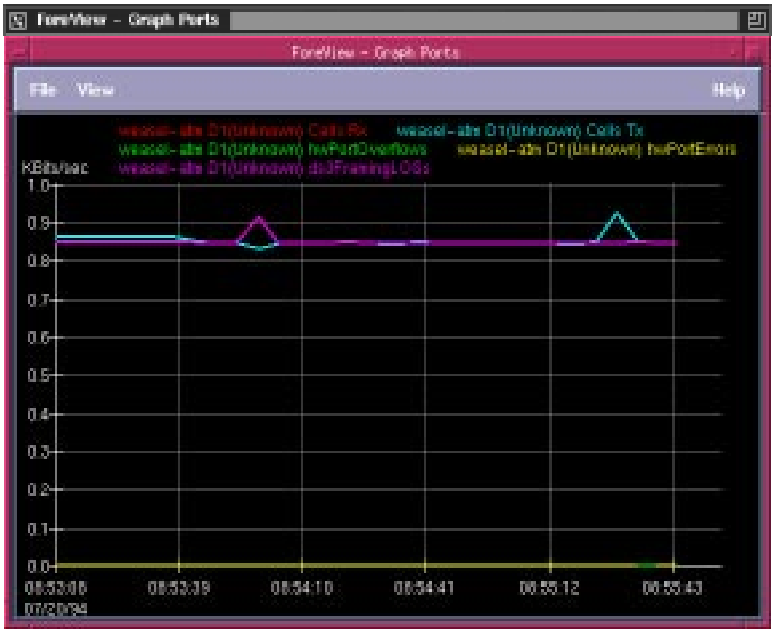

ForeView - Graph Ports
ForeView - Graph Ports
File
View
Help
weasel- atm D1(Unknown) Cells Rx
weasel- atm D1(Unknown) Cells Tx
weasel- atm D1(Unknown) hwPortOverflows
weasel- atm D1(Unknown) hwPortErrors
weasel- atm D1(Unknown) ds3FramingLOSs
KBits/sec
1.0
0.9
0.8
0.7
0.6
0.5
0.4
0.3
0.2
0.1
0.0
08:52:08
07/20/94
08:52:39
08:54:10
08:54:41
08:55:12
08:55:43

Figure 11.4 - Cell Loss, Framing Error

Cell loss may also be caused by a *noisy* or *dirty* line. To check for this effect, look at the **Hardware Errors** counter which is reported in the **Port Status** screen within the Front Panel. Line-specific error statistics which are collected for DS-3, E-3, and OC-x switch ports may also be checked. These appear at the bottom of the Front Panel's **Port Status** screen.

In addition to cell loss, another performance statistic that channel trace graphs can show is the number of rejects caused by bandwidth policing in a network. When graphing both rejects and cells, normally the rejects at all hops should track at zero. If rejects increase from zero, there should be a corresponding decrease in the cell flow at the hop where policing is occurring.

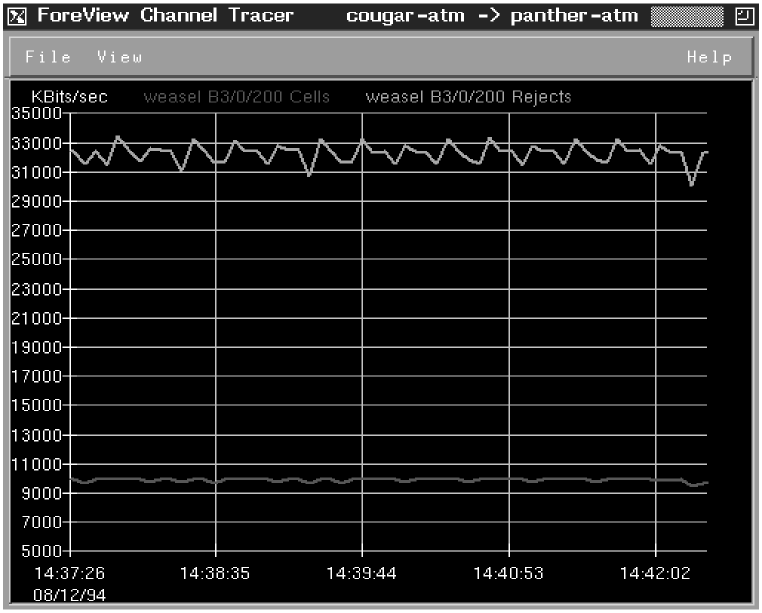


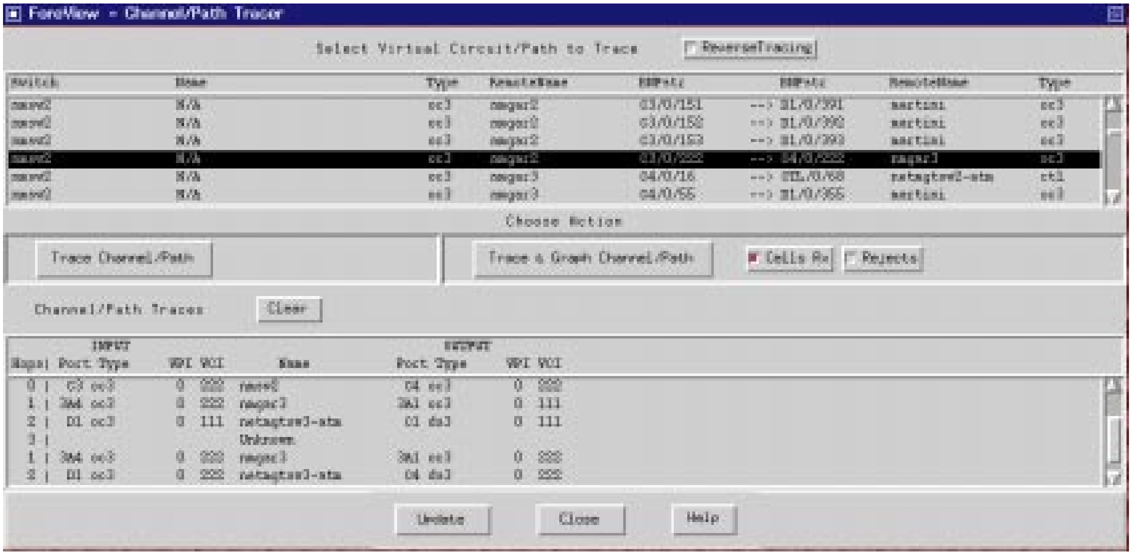
Figure 11.5 - Policing Graph

FORE switches can be configured to tag or reject cells when contract bandwidth is exceeded. You can change a switch's policing to tag or reject cells that exceed contract bandwidth using the ATM Management Interface (**`AMI`**) on the switch. Tagging cells sets Cell Loss Priority (CLP) bit in cells over contract bandwidth, giving them lower priority. Rejecting cells causes the switch to drop all cells above the contract bandwidth.

The policing bandwidth is specified when a channel is created. When establishing PVCs or SPVCs with ForeView's PVC and SPVC tools, bandwidth must be specified. On an ASX-200, this bandwidth is policed in hardware and if bandwidth is exceeded, the configured action takes place. Specifying a bandwidth of 0 disables policing and allows the channel to use all available bandwidth. SVCs created by SPANS use bandwidth 0.

11.2.4 Point-to-Multipoint Traces

The examples shown so far in this chapter depict point-to-point channels in an ATM network. FORE switches and adapters also support both point-to-multipoint and multipoint-to-point channels. The Channel/Path Tracer can also trace these types of channels. To trace a point-to-multipoint channel, find and select the channel in your network as you would a point-to-point channel. Figure 11.6 shows a trace of a point-to-multipoint channel.



```
Switch   Name   Type   RemoteName   PP/vc        PP/vc        RemoteName      Type
masw2    N/A    oc3    nmgsr2       C3/0/151 --> D1/0/391     martini         oc3
masw2    N/A    oc3    nmgsr2       C3/0/152 --> D1/0/392     martini         oc3
masw2    N/A    oc3    nmgsr2       C3/0/153 --> D1/0/393     martini         oc3
masw2    N/A    oc3    nmgsr2       C3/0/222 --> 04/0/222     nmgsr3          oc3
masw2    N/A    oc3    nmgsr3       04/0/16  --> CTL/0/68     netagtsw2-atm   ctl
masw2    N/A    oc3    nmgsr3       04/0/55  --> D1/0/355     martini         oc3
```

```
        INPUT                                     OUTPUT
Hops| Port Type    VPI VCI        Name          Port Type    VPI VCI
  0 |   C3 oc3      0  222   masw2                C4 oc3      0  222
  1 |  3A4 oc3      0  222   nmgsr3              3A1 oc3      0  111
  2 |   D1 oc3      0  111   netagtsw3-atm        C1 ds3      0  111
  3 |                        Unknown
  1 |  3A4 oc3      0  222   nmgsr3              3A1 oc3      0  222
  2 |   D1 oc3      0  222   netagtsw3-atm        C4 ds3      0  222
```

Figure 11.6 - Point-to-Multipoint Channel

There is one caveat to tracing point-to-multipoint channels. Tracing will show only those points that are directly involved from the point the trace was initiated. That is, all links that contribute cells to this link on the upstream and all those points that receive cells from this link on the downstream will be included in the trace.

You will only see multipoint ***fanouts*** downstream from the trace point that you choose. If you trace the following point-to-multipoint connection at the indicated point, you will not see the dashed legs of the connection in your trace.

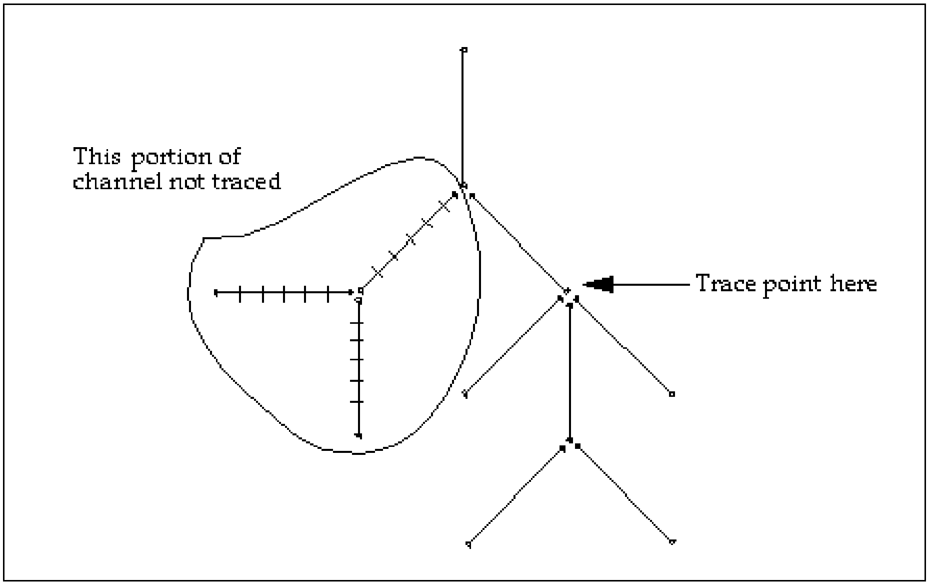


Figure 11.7 - Fanout of Partial Downstream Trace

Selecting a trace point upstream at this indicated point will trace the entire connection.

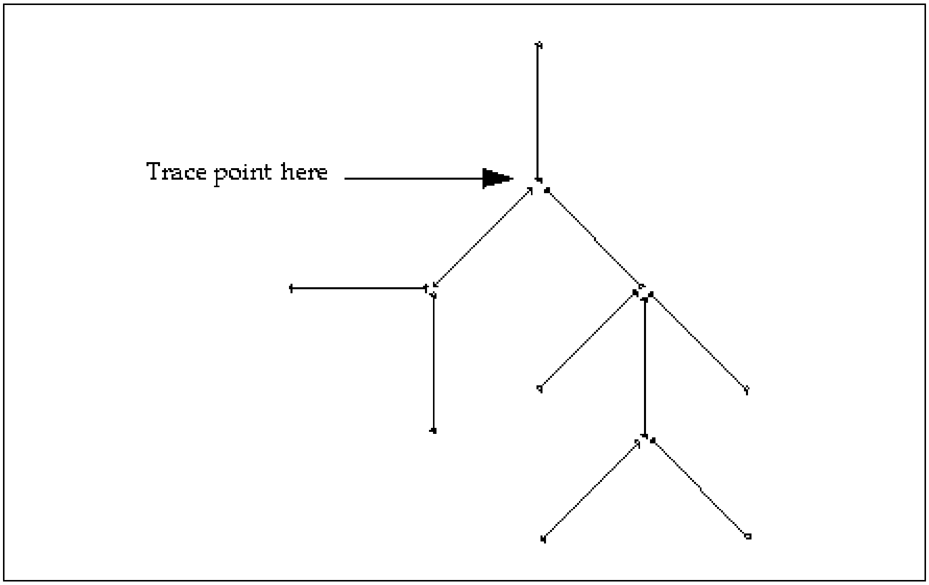
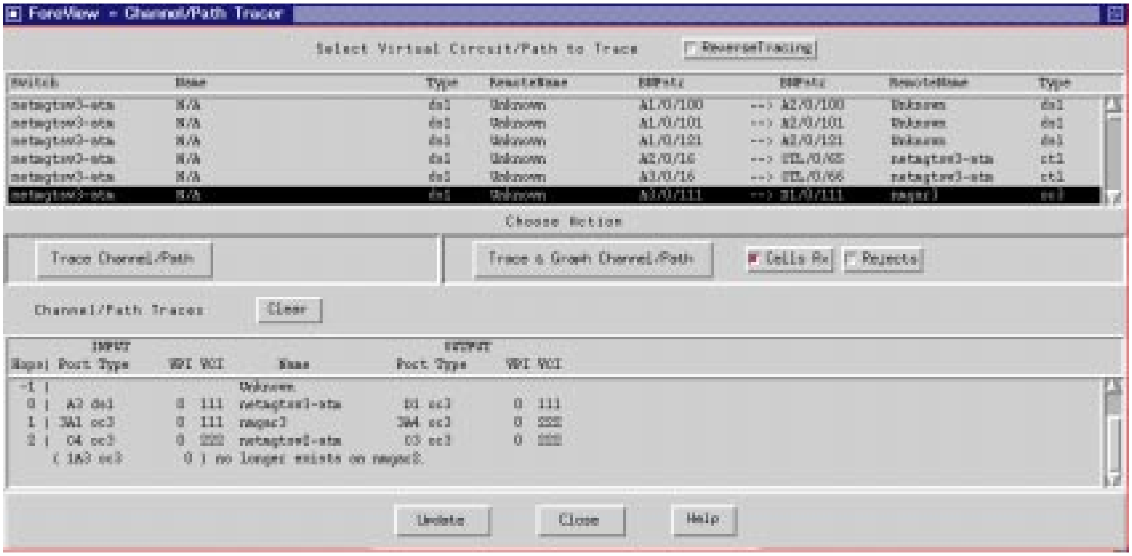


Figure 11.8 - Fanout of Complete Trace

11.2.5 Multipoint-to-Point Traces

Tracing multipoint-to-point connections is also supported by **`fvtracer`**. Figure 11.9 shows a trace of a multipoint-to-point network.



ForeView - Channel/Path Tracer

Select Virtual Circuit/Path to Trace □ ReverseTracing

Switch	Name	Type	RemoteName	SWPort		SWPort	RemoteName	Type
netmgtsw3-atm	N/A	ds1	Unknown	A1/0/100	-->	A2/0/100	Unknown	ds1
netmgtsw3-atm	N/A	ds1	Unknown	A1/0/101	-->	A2/0/101	Unknown	ds1
netmgtsw3-atm	N/A	ds1	Unknown	A1/0/121	-->	A2/0/121	Unknown	ds1
netmgtsw3-atm	N/A	ds1	Unknown	A2/0/16	-->	CTL/0/65	netmgtsw3-atm	ctl
netmgtsw3-atm	N/A	ds1	Unknown	A3/0/16	-->	CTL/0/66	netmgtsw3-atm	ctl
netmgtsw3-atm	N/A	ds1	Unknown	A3/0/111	-->	B1/0/111	nmgsc3	oc3

Choose Action

Channel/Path Traces

```
              INPUT                                   OUTPUT
Hops| Port Type      VPI VCI         Name           Port Type      VPI VCI
 -1 |                          Unknown
  0 |   A3 ds1         0  111  netmgtsw3-atm          B1 oc3         0  111
  1 |  3A1 oc3         0  111  nmgsc3                3A4 oc3         0  222
  2 |   C4 oc3         0  222  netmgtsw2-atm          C3 oc3         0  222
      ( 1A3 oc3          0 ) no longer exists on nmgsc3.
```

Figure 11.9 - Multipoint-to-Point Trace

As with point-to-multipoint, only the links that either contribute cells to the point (link) that was traced, or links that receive cells from the point (link) that was traced are included in the trace output. You will only see ***fanins*** upstream from the trace point that you choose. If you trace the following point-to-multipoint connection at the indicated point, you will not see the dashed legs of the connection in your trace.

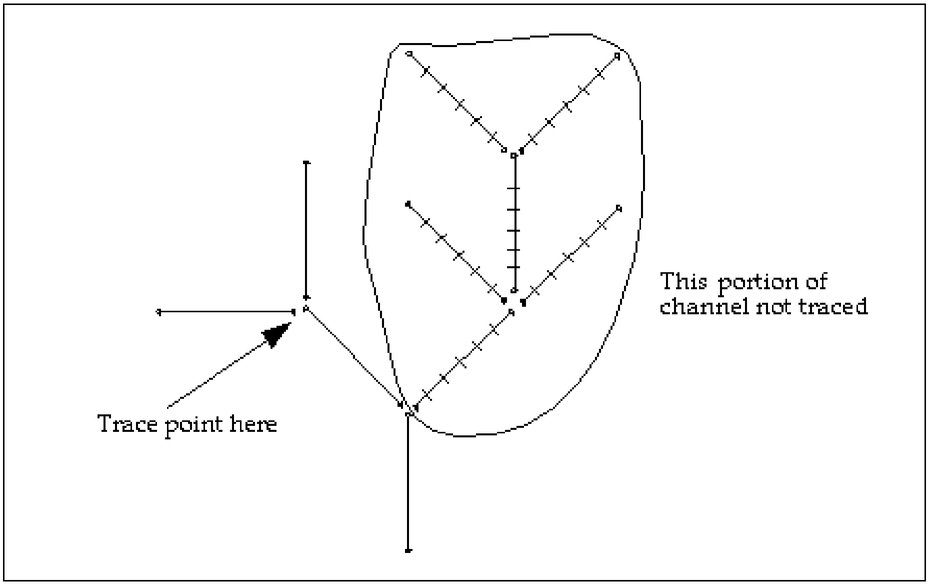


Figure 11.10 - Fanin of Partial Upstream Trace

Selecting a trace point downstream at this indicated point will trace the entire connection, because all the links above it can contribute cells.

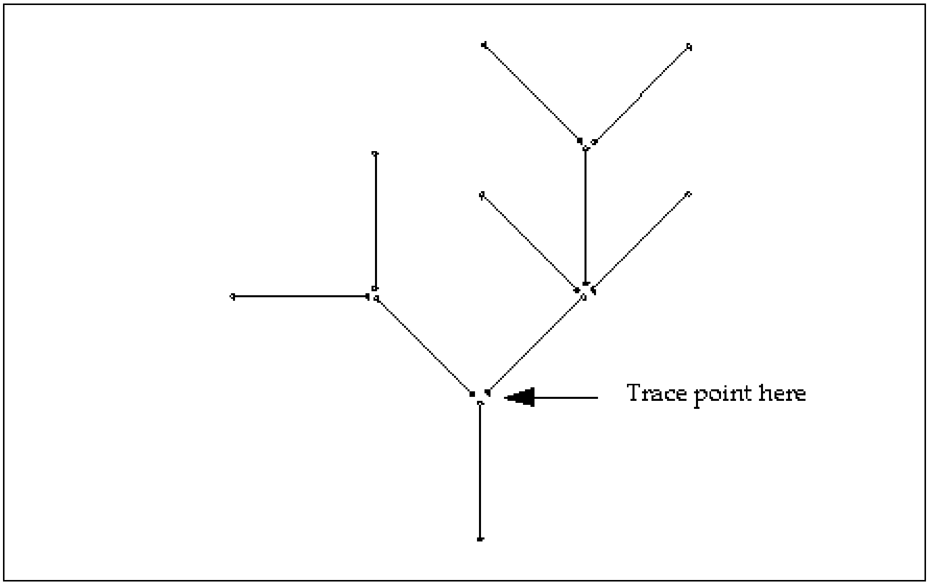
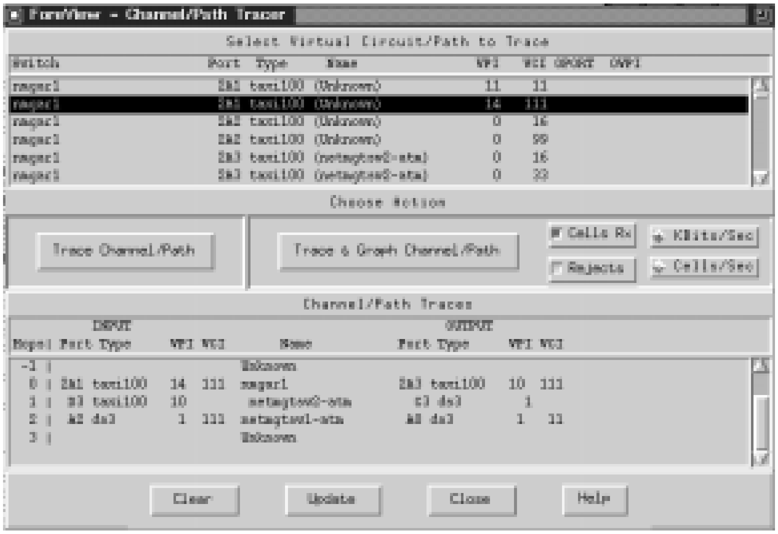


Figure 11.11 - Fanin of Entire Trace

11.2.6 Tracing Through a PVP

Tracing channels through a PVP (Through Path) is now supported by **`fvtracer`**. Figure 11.12 shows a trace of a channel through a PVP.



```
Switch                Port  Type     Name                 VPI   VCI  OPORT  OVPI
nmgar1                 2A1  taxi100  (Unknown)             11    11
nmgar1                 2A1  taxi100  (Unknown)             14   111
nmgar1                 2A2  taxi100  (Unknown)              0    16
nmgar1                 2A2  taxi100  (Unknown)              0    99
nmgar1                 2A3  taxi100  (netmgtsw2-atm)        0    16
nmgar1                 2A3  taxi100  (netmgtsw2-atm)        0    33
```

```
          INPUT                                       OUTPUT
Hops| Port Type      VPI VCI      Name             Port Type      VPI VCI
  -1 |                           Unknown
   0 | 2A1 taxi100    14  111   nmgar1            2A3 taxi100    10  111
   1 |  D3 taxi100    10         netmgtsw2-atm      C3 ds3          1
   2 |  A2 ds3         1  111   netmgtsw1-atm      A0 ds3          1   11
   3 |                           Unknown
```

Figure 11.12 - Tracing Through a PVP

Here we see PVC of unknown origin that enters a switch **`nmgar1`** using **`VPI/VCI 14/111`** on port **`2A1`**. The PVC exits the switch using **`VPI/VCI 10/111`** on port **`2A3`**. This connection is traced to **`netmgtsw2-ATM`**, where it enters on port **`D3`** and is assigned to PVP **`10`**. You can see the connection exit **`netmgtsw2-ATM`** on PVP **`1`**. Entering switch **`nmsw1`** on **`A2/1/111,`** it exits the switch on **`A0/1/11`**. Notice that the connection maintains its VCI value of 111 when it exits the PVP on switch **`netmgtsw1`**

11.3 Tracing from the Command-line

For convenience, *ForeView*’s Channel/Path Tracer can be run from the command-line of your operating system. The following explains the command-line syntax:

fvtracer *switch [switch]...*

fvtracer *switch:port_identifier/VPI/VCI [switch:port_identifier/VPI/VCI]...*

where: switch is the IP hostname or ATM address of a switch in a ForeRunner ATM network or a link identifier in the format <switch_hostname>:<port_identifier>. *port_identifier* is the nomenclature used by all the ForeView and ForeRunner tools to identify ports. Example: For the first port in network module "C" in an ASX-200, the port identifier is C1. *VPI/VCI* is the Virtual Path Identifier and Virtual Channel Identifier respectively.

CHAPTER 12 Taking Inventory of ATM Equipment

ForeView provides a utility to keep an inventory of all the ATM equipment found in your network, including switches, hosts, network modules, and LAN-access devices such as the ES-3810. This utility also provides the means to sort the information by rearranging the display columns, and also provides a user-configurable filter option that allows you to take inventory of specific subsets of you network equipment. The Inventory utility runs on all *ForeView* platforms, including the Stand-alone network map. This chapter provides information on how to use the Inventory utility.

12.1 Launching the Inventory Utility

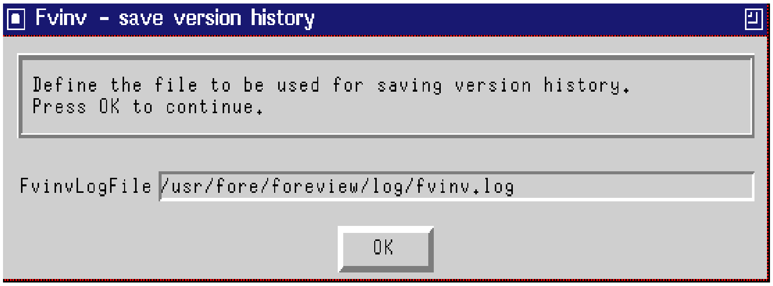
The Inventory utility can be launched from *ForeView* running under HP OpenView, SunNet Manager, and the Stand-alone Map. To launch the Inventory utility, select the desired network entities (switches, hosts, LAN-access devices) and do the following:

- From HP OpenView or NetView for AIX, pull down the *ForeView* menu and select **`Inventory`**.
- From SunNet Manager, pull down the Tools menu and select **`ForeView Inventory`**.
- From the Stand-alone Map, pull down the **`Tools`** menu and select **`Inventory`**.
- From the command line, type **`fvinv`** to launch the Inventory utility.

12.1.1 Defining the Version History File

The inventory utility keeps track of the version history of *ForeThought* software running on your ATM switches. This information is stored in a version history file. This file can be defined in the *ForeView* configuration file. The default version history file is **`usr/fore/foreview/log/fvinv.log`**. You may define a different version history file by entering a file name after the **`FvinvConfFile`** line in the *ForeView* configuration file.

If you fail to define a version history file in the *ForeView* configuration file, you will be prompted for a file name every time you run the inventory utility. The prompt for the version history file will appear, similar to the one shown in Figure 12.1.



```
Define the file to be used for saving version history.
Press OK to continue.
```

FvinvLogFile /usr/fore/foreview/log/fvinv.log

Figure 12.1 - Version History File Name Prompt

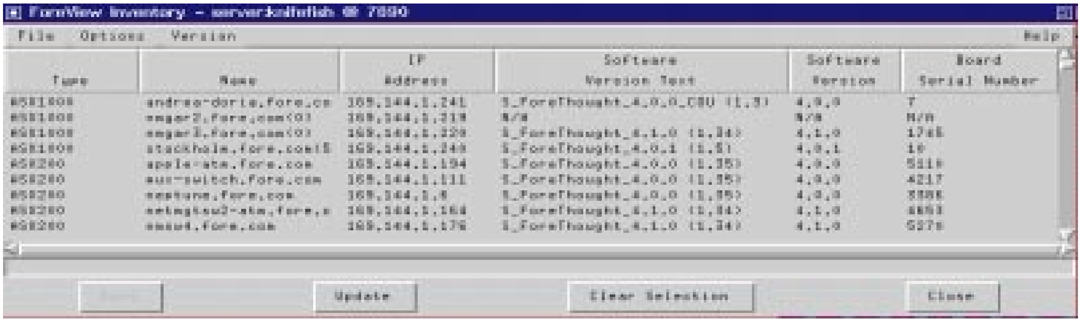
NOTE The version history file is updated each time you perform inventory management tasks.

12.2 The Inventory Dialog

After defining a version history file name (if applicable), the Inventory dialog appears, similar to the one shown in Figure 12.2. To view the software version history for one or more devices, select devices from the inventory list. To save the current inventory information to a file, select the **Save As...** option from the **File** menu.

NOTE

To select more than one item, hold down the **Ctrl** key, and click on the item with the left mouse button.



Type	Name	IP Address	Software Version Text	Software Version	Board Serial Number
ASX1000	andrea-doria.fore.co	169.144.1.241	S_ForeThought_4.0.0_CBU (1.3)	4.0.0	7
ASX1000	engar2.fore.com(0)	169.144.1.219	N/A	N/A	N/A
ASX1000	engar1.fore.com(0)	169.144.1.220	S_ForeThought_4.1.0 (1.34)	4.1.0	1766
ASX1000	stockholm.fore.com(5	169.144.1.249	S_ForeThought_4.0.1 (1.5)	4.0.1	19
ASX200	apple-atm.fore.com	169.144.1.194	S_ForeThought_4.0.0 (1.35)	4.0.0	5116
ASX200	aus-switch.fore.com	169.144.1.111	S_ForeThought_4.0.0 (1.35)	4.0.0	4217
ASX200	neptune.fore.com	169.144.1.6	S_ForeThought_4.0.0 (1.35)	4.0.0	5586
ASX200	netmgtsw2-atm.fore.c	169.144.1.164	S_ForeThought_4.1.0 (1.34)	4.1.0	4653
ASX200	mssw4.fore.com	169.144.1.176	S_ForeThought_4.1.0 (1.34)	4.1.0	5279

Figure 12.2 - The Inventory Dialog

12.2.1 Inventory Options

The Inventory application provides an **Options** pull-down for sorting order and filters that allow you to customize the inventory to your specific needs.

The **Sort Decreasing** option can be turned on or off by clicking on the menu item. A red button indicates that the sort is in decreasing order.

The **Filters** option can be used to manipulating the data to present a particular view of the inventory. The use of filters is covered in the next section.

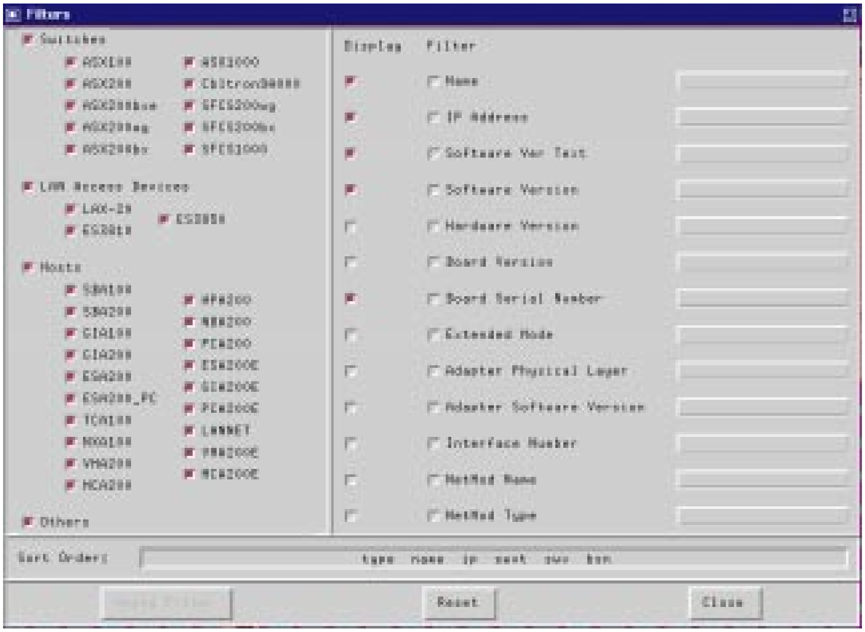
12.3 Filtering

The Inventory application provides filters that allow you to take inventory of specific network entities. Filters can be turned on or off for the following devices:

- Switches
- Network modules, interfaces
- LAN access devices
- Hosts
- Others (non-FORE equipment)

Filters are used to alter the way the information is displayed. Therefore, filters are useful only after the inventory of devices is taken. Filters do not affect inventory gathering. They are useful for manipulating the data to present a particular view of the inventory.

To configure the filter options, pull down the **`Options`** menu from the Inventory front panel (Figure 12.2) and select **`Filters`**. The Filters dialog is shown below.



☒ Switches
- ☒ ASX100
- ☒ ASX200
- ☒ ASX200bxe
- ☒ ASX200wg
- ☒ ASX200bx
- ☒ ASX1000
- ☒ Cabletron9A000
- ☒ SFCS200wg
- ☒ SFCS200bx
- ☒ SFCS1000

☒ LAN Access Devices
- ☒ LAX-20
- ☒ ES3810
- ☒ ES3850

☒ Hosts
- ☒ SBA100
- ☒ SBA200
- ☒ GIA100
- ☒ GIA200
- ☒ ESA200
- ☒ ESA200_PC
- ☒ TCA100
- ☒ MXA100
- ☒ VMA200
- ☒ HCA200
- ☒ HPA200
- ☒ NBA200
- ☒ PCA200
- ☒ ESA200E
- ☒ GIA200E
- ☒ PCA200E
- ☒ LANNET
- ☒ PMA200E
- ☒ HCA200E

☒ Others

Display	Filter
☒	☐ Name
☒	☐ IP Address
☒	☐ Software Ver Text
☒	☐ Software Version
☐	☐ Hardware Version
☐	☐ Board Version
☒	☐ Board Serial Number
☐	☐ Extended Mode
☐	☐ Adapter Physical Layer
☐	☐ Adapter Software Version
☐	☐ Interface Number
☐	☐ NetMod Name
☐	☐ NetMod Type

Sort Order: type name ip swvt swv bsn

Figure 12.3 - Filtering Options

12.3.1 Filtering by Device or Host Type

To filter by device or host type, select the device or host type from the appropriate lists. You can filter using a combination of device and host types.

When using filters, remember the following points:

- A red button indicates that the item type is part of the inventory.
- When you click **OFF** the red button on Switches, LAN Access Devices, Hosts, and Others, all items under those headings are also turned off.
- To add individual items to the inventory, click **ON** the red button for those items.

12.3.2 Filtering by Names and Versions

To filter by device names, IP addresses, or software versions, select the appropriate item or items from the **Filter** column at the right of the **Filters** dialog. You can filter using a combination of the items in the selection column.

When using names and version numbers as filters, remember the following points:

- A red button next to an item in the **Filter** column indicates that the item is part of the inventory display.
- When you click **ON** the red button at any item in the **Filter** column, the entry field to the right of the item is active. Enter the string for the inventory filter in the field.

12.4 Sorting

To sort the inventory of devices and/or host types, use the **`Sort`** button at the bottom of the Inventory front panel.

When sorting, remember the following points:

- The fields displayed on the front panel are selected from the Filters dialog.
- The Inventory utility sorts items from left to right across the columns on the front panel. The sorting is increasing by default.
- Move the columns to change the sort order (see section 12.4.2). Sorting begins at the left-most column on the front panel.
- When you click **`ON`** the red button on the **`Sort Decreasing`** selection, the items in the front panel are re-sorted.

12.4.1 Sort Order

The sort order can be viewed in the `SortOrder:` field located at the bottom of the Filters dialog. The items that appear in this field are selected from the display column (see Figure 12.3).

When selecting display items, remember the following points:

- A red button indicates that the item is part of the Inventory front panel display (Figure 12.3).
- The order in which the items appear in the Display list is not necessarily the order you will see on the Inventory front panel.
- The order of the Inventory front panel can be re-arranged by moving columns.

12.4.2 Moving Columns

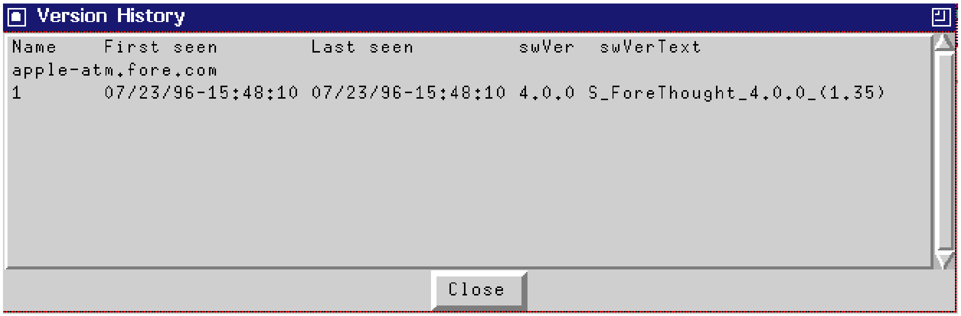
The order of the Inventory front panel can be re-arranged by moving columns. Items that appear in the front panel are selected from the **`Filters`** dialog. The selection of the items is independent of their order in the Inventory front panel. The **`SortOrder:`** field located at the bottom of the **`Filters`** dialog lists the order of the items that appear in the Inventory front panel.

When moving columns, remember the following points:

- Select the column you want to move by clicking on the header of the column. You will see the message “move selected column to ... (press on desired position)”.
- Position the cursor on the column header where you want to place the selected column and click the mouse button. This action places the selected column in this new position. The other columns are displaced one position to the left or right.
- The **`Sort`** button becomes active when you move a column. To perform the sort, select the **`Sort`** button after you have finished rearranging the columns.

12.5 Version History

To view the software version history of devices and/or host types, pull down the **Version** menu from the Inventory dialog (Figure 12.2) and select **History**. An example of the History dialog is shown below.



```
Name     First seen         Last seen          swVer   swVerText
apple-atm.fore.com
1        07/23/96-15:48:10 07/23/96-15:48:10 4.0.0  S_ForeThought_4.0.0_(1.35)
```

Figure 12.4 - Version History Dialog

When viewing the version history, remember the following points:

- The version history shows the time stamp of the current software and the last time the version was checked.
- If the software for any device is upgraded, an new entry is added to the version history file with the time stamp of the new software version. The original entry for the previous version of software remains in the file.

12.6 Inventory from the Command-line

For convenience, *ForeView*'s Inventory utility can be run from the command-line of your operating system. The following explains the command-line syntax:

fvinv *[-cw write_community] [-cr read_community] [hostname ...]*

WHERE *hostname* is the IP hostname of a host, switch, or access device in a *ForeRunner* ATM network.

CHAPTER 13 OAM Management

OAM cells provide a means to support fault and performance management at the ATM layer. The OAM capability on FORE ATM switches provides a means to propagate information regarding fault condition in the ATM network. The *ForeView* OAM capability provides the mechanism for end users to activate OAM cell flow on a FORE ATM switch, to receive indication of OAM cells flow activity, and to monitor the ATM layer utilizing OAM cell flow.

13.1 Introduction

The generation of AIS/RDI (Alarm Indication Signal)/(Remote Defect Indication) OAM cells is supported for VPs (virtual paths) and VCs (virtual channels), including through paths, originating paths, PVCs, and PNNI SPVCs that originate on a port.

NOTE

The *ForeThought* 4.1 release is limited to a maximum of five terminating virtual paths per interface supporting RDI OAM cell generation and a maximum of fifty virtual connections (VPs and VCs) per interface supporting AIS OAM cell generation.

For terminating virtual paths on a given port, F4 (VP) RDI OAM cells are generated under the following conditions:

- OAM cell generation is enabled on that port
- A physical layer failure (loss of carrier, loss of frame, etc.) occurs on the receive side of the port, or an F4 (VP) AIS cell arrives on the receive side of the port

For non-terminating virtual paths, F4 (VP) AIS OAM cells are generated under the following conditions:

- OAM cell generation is enabled downstream on the transmit port
- A physical layer failure (loss of carrier, loss of frame, etc.) occurs in the receive port of the virtual path

For non-terminating virtual channels, F5 (VC) AIS OAM cells are generated under the following conditions:

- OAM cell generation is enabled on the downstream transmit port
- A physical layer failure (loss of carrier, loss of frame, etc.) occurs on the receive port of the channel, or an F4 (VP) AIS condition is present on the receive port of the virtual path

An AIS is sent in the downstream direction (away from the failure). Receiving an AIS cell indicates that a physical layer failure condition is present upstream from the receiver. An RDI cell is sent toward the failure when a physical fault or AIS condition is detected on the terminating virtual path. Receiving a RDI cell indicates that a fault exists in the transit pathway of the virtual connection described by the RDI cell.

NOTE

Currently, AIS/RDI OAM cell generation is supported only for point-to-point connections.

The following table summarizes the physical layer receive path failures. The presence of one or more of these indications on a physical interface is sufficient to actuate OAM activity for the incoming virtual connections on that port.

Network Module Type:	Physical Layer Alarm Indications:
ASX-1000 Backplane	Loss of carrier
DS-1	Loss of carrier, LOF, LOS, AIS, PLCP LOF
DS-3	Loss of carrier, LOF, LOS, AIS, PLCP LOF
E-1	Loss of carrier, OOF, OOCMF, LOF, LOS, AIS, TS16 AIS
E-3	Loss of carrier, LOF, LOS, LCD, AIS
J-2	Loss of carrier, LOC, LOF, LOS, AIS
OC-x	Loss of carrier, Section LOF, Section LOS, Line AIS, Path AIS, Path LOP
TAXI	Loss of carrier
TP-25	Loss of carrier

NOTE

Definitions for any of the above alarm indicators can be found in the respective port configuration sections in Chapter 8.

13.2 OAM Capabilities

ForeView uses the OAM feature as a means to troubleshoot network problems. The OAM feature provides:

- The mechanism to activate/deactivate OAM cell generation on a per port basis, and
- The mechanism to monitor OAM cell flow activity on a per port (or switch) basis.

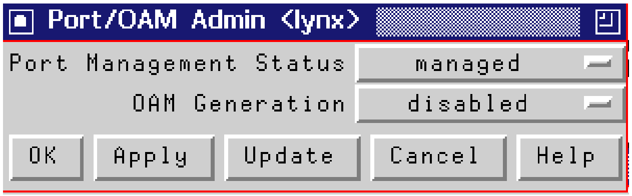
The following sequence of events describes the activities an end user would typically perform to take advantage of this design:

1. Activate OAM generation on ports from selected FORE ATM switches supporting OAM. This will enable OAM cell flow from these ports whenever a fault is detected by the switch. This is will also trigger FORE ATM switch supporting OAM to generate OAM traps.
2. Launch the network manager event browser and look for OAM traps.
3. Using the OAM traps as a cue, activate the OAM switch monitor to aid in narrowing down the source of the fault, as well as to gauge the effect of the fault condition on various part of the network.

13.2.1 OAM Cell Generation Activation

The *ForeView* user interface allows network managers to activate or deactivate OAM cell generation on a port-by-port basis in FORE ATM switches supporting OAM. From a *ForeView* front panel, pull down the Configure menu and select Port -> Port/OAM Admin.

This launches the per-port OAM administration dialog, as illustrated below.



Port Management Status: managed
OAM Generation: disabled

Figure 13.1 - OAM Administration Dialog

The dialog options are defined as follows:

Port Management Status Toggled variable indicating whether the port is managed or unmanaged.

OAM Generation Indicates whether OAM cell generation is enabled or disabled for the selected port(s). When a user toggles the OAM Generation, an SNMP command is sent to the switch to activate/deactivate OAM cell generation on the selected port(s). Once enabled, (F4/F5 AIS and F4 RDI) cells (whichever is applicable) will be generated on the port(s) whenever valid conditions exist. Transmitted/Received OAM cells will be counted, and a time stamp is maintained on the switch.

NOTE

Note that this dialog does not affect the switch's ability to receive, time stamp and count incoming OAM cells. Port/OAM administration will be disabled on a FORE ATM switch not supporting OAM.

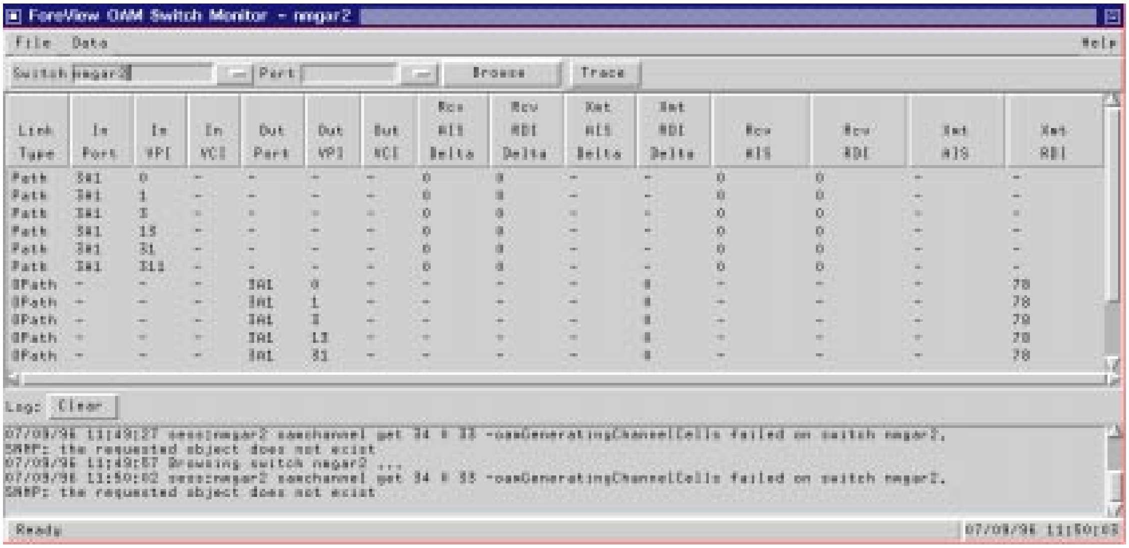
13.2.2 OAM Switch Monitor

The *ForeView* OAM Switch Monitor application provides the mechanism to view and monitor F4/F5 OAM cell activities in and out of a FORE ATM switch. It will poll a designated switch for all outstanding cell flow counters in the OAM MIB tables and display the latest F4/F5 OAM information in a list box. The user will be able to detect at a glance at which Port/VP/VC F4/F5 OAM cells flowed in and out of the switch.

This application can be launched from the Front Panel, or the Port Control dialog, or directly from the command line. From the command line, the application is invoked using the following command line syntax:

```
fvoams <switch> -port [<port>] [-poll <interval>]
```

The <port> argument when given restricts the display to F4/F5 OAM information to that port. Otherwise, all available OAM information on the switch is presented.



Link Type	In Port	In VPI	In VCI	Out Port	Out VPI	Out VCI	Rcv AIS Delta	Rcv RDI Delta	Xmt AIS Delta	Xmt RDI Delta	Rcv AIS	Rcv RDI	Xmt AIS	Xmt RDI
Path	3A1	0	-	-	-	-	0	0	-	-	0	0	-	-
Path	3A1	1	-	-	-	-	0	0	-	-	0	0	-	-
Path	3A1	3	-	-	-	-	0	0	-	-	0	0	-	-
Path	3A1	13	-	-	-	-	0	0	-	-	0	0	-	-
Path	3A1	31	-	-	-	-	0	0	-	-	0	0	-	-
Path	3A1	311	-	-	-	-	0	0	-	-	0	0	-	-
OPath	-	-	-	3A1	0	-	-	-	-	0	-	-	-	78
OPath	-	-	-	3A1	1	-	-	-	-	0	-	-	-	78
OPath	-	-	-	3A1	3	-	-	-	-	0	-	-	-	79
OPath	-	-	-	3A1	13	-	-	-	-	0	-	-	-	78
OPath	-	-	-	3A1	31	-	-	-	-	0	-	-	-	78

```
07/09/96 11:49:27 sess:nmgar2 oamchannel get 34 0 33 -oamGeneratingChannelCells failed on switch nmgar2,
SNMP: the requested object does not exist
07/09/96 11:49:57 Browsing switch nmgar2 ...
07/09/96 11:50:02 sess:nmgar2 oamchannel get 34 0 33 -oamGeneratingChannelCells failed on switch nmgar2,
SNMP: the requested object does not exist
```

Ready   07/09/96 11:50:03

Figure 13.2 - OAM Switch Monitor Dialog

The dialog columns are defined as follows:

Link Type Indicates the type of channel generating the OAM cells, OAM cells will be generatedfor through paths and originating paths, through channels (PVCs), and PNNI SPVCs that originate on that port.

In Port/VPI/VCI The source port, VP, and VC.

Out Port/VPI/VCI The destination port, VP, and VC.

Rcv AIS Delta The Rcv AIS Delta shows the change in this OAM counter value since the last polling cycle.

Rcv RDI Delta The Rcv RDI Delta shows the change in this OAM counter value since the last polling cycle.

Xmt AIS Delta The Xmt AIS Delta shows the change in this OAM counter value since the last polling cycle.

Xmt RDI Delta The Xmt RDI Delta shows the change in this OAM counter value since the last polling cycle.

Rcv AIS The Rcv AIS (Alarm Indication Signal) indicates the number of AIS cells received on that port. AIS cells are sent in the downstream direction (away from the failure), then receiving an AIS cell indicates that a physical layer failure condition is present upstream from the receiver.

Rcv RDI The Rcv RDI (Remote Defect Indication) indicates the number of RDI cells received on that port. RDI cells are sent upsteam (toward the failure) when a physical fault or AIS condition is detected on a terminating through path, then receiving a RDI cell indicates that a fault exists downstream in the transit pathway of the virtual connection described by the RDI cell.

Xmt AIS The Xmt AIS (Alarm Indication Signal) indicates the number of AIS cells transmitted on that port. The AIS cells are transmitted downstream from the point of failure.

Xmt RDI The Xmt RDI (Remote Defect Indication) indicates the number of RDI cells transmitted on that port. The RDI cells are transmitted upstream toward the source of failure.

13.2.3 Menu Bar

The menu bar at the top of the OAM Switch Monitor provides the following controls and commands:

13.2.3.1 File

File / Quit Closes the OAM Switch Monitor application.

13.2.3.2 Data

Use the Data menu to set the polling interval, browse selected switches, and launch traces of problem links. Options are:

Data /Polling The OAM Switch Monitor will periodically poll a switch for status updates. The polling interval can be changed by using the Polling menu. The default polling interval is every 30 seconds, but can be changed to 10 or 60 seconds. Polling can also be turned off through this menu.

Data /Browse The Browse function scans the links on the selected switch, including incoming and outgoing paths and channels and the corresponding OAM cells generated.

This function also is available via the Browse button. The scope of the browsing can be modified by selecting a switch or an available port and then selecting Browse.

Data /Trace The Trace function traces the selected link to aid in narrowing down the source of the fault. The output of the trace is displayed in the log window.

This function also is available via the Trace button.

13.2.3.3 Help

Launches the on-line help for the OAM Switch Monitor.

13.3 OAM Monitoring from the Command-line

For convenience, *ForeView*'s OAM Switch Monitor can be run from the command-line of your operating system. The following explains the command-line syntax:

fvoams *[switch] [-port <portnum>] [-poll <interval>] [-cr <community>]*

WHERE *switch* is the name of the switch to browse for OAM F4/F5 cells; *–port<portnum>* is the port number on the switch to browse for OAM F4/F5 cells (if this option is not provided, OAM counters for all ports on the switch will be retrieved); *–poll<interval>* is the polling interval to use between auto browse; *–cr<community>* specifies the SNMP read community string to use when retrieving OAM F4/F5 information from the switch.

CHAPTER 14 Call Record and Performance Monitoring

ForeView supports call record and performance monitoring data collection for billing and connection performance monitoring. These capabilities are implemented through a combination of *ForeRunner* switch support and *ForeView* management application support.

14.1 General Functionality

The call record and performance monitoring data collection is composed of two independent applications sharing a common management and data transfer interface.

The call record data collection application is responsible for managing call records for connections. Call records are created at connection establishment time and transmitted to a data collection server at the end of a collection interval.

The performance monitoring data collection application is responsible for managing performance records for equipment and transmission facility resources. At the end of a collection interval, this application will read all the applicable counters and registers, and then transmit the data to a data collection server.

14.1.1 Call Record Data Collection

The call record data collection application supports call record generation for calls established via management configuration (PVCs, PVPs, and Smart PVCs created under the SPANS PNNI) or through UNI signalling (SVCs).

NOTE

There is no call record support for calls established through SPANS NNI signalling.

The call record process can be summarized as follows:

- A call record is created upon connection establishment.
- At the end of a collection interval, call records are transmitted to a data server.

NOTE

For successful file transfer in the Windows NT environment, make sure that the Windows FTP Server is installed in the network configuration.

- Call records contain the full context associated with a new connection established during the collection interval, or an on-going connection, or a connection which terminated during the collection interval, or a connection that was established and terminated during the collection interval.

14.1.2 Performance Monitoring Data Collection

The performance monitoring data collection application is responsible for collecting performance usage measurements for the following equipment and transmission facility resources associated with each switch fabric:

- Fabric board number
- Network module type
- Port number

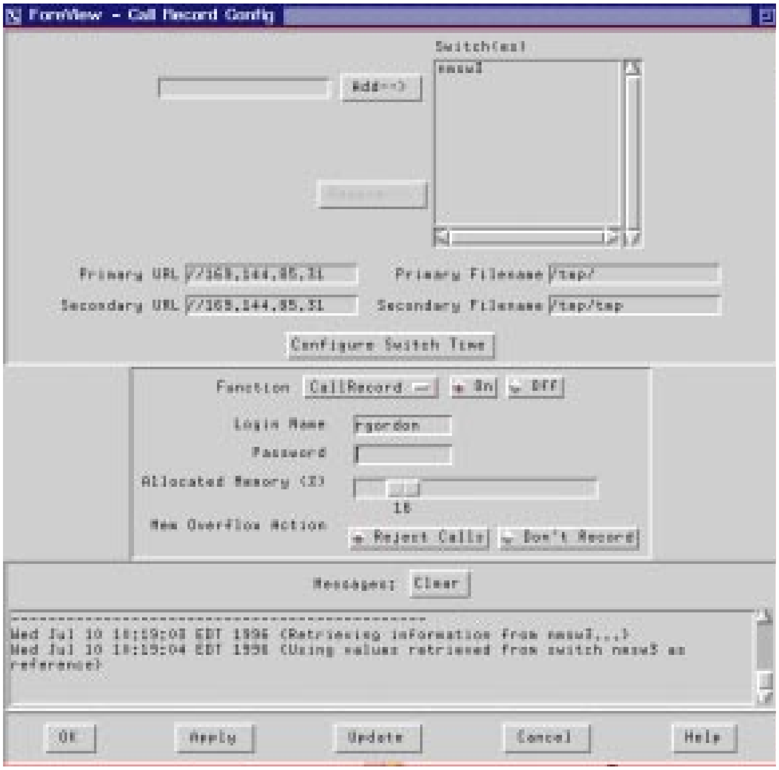
At the end of a collection interval, the performance monitoring application will determine the current equipment configuration, create a file in memory, and take a snapshot of counters and registers for each configured resource. This file is then sent to a data server.

NOTE

For successful file transfer in the Windows NT environment, make sure that the Windows FTP Server is installed in the network configuration.

14.2 The Call and Performance Record Configuration Interface

The *ForeView* call record and performance monitoring application is designed to let the user configure call records and performance monitoring data for billing purposes. This application can be launched from the Front Panel or directly from the command line by invoking the command **`fvcall`**. This launches the Call Record Config dialog, as illustrated below.



Switch(es): nmsw3

Primary URL //169.144.85.31
Secondary URL //169.144.85.31
Primary Filename /tmp/
Secondary Filename /tmp/tmp

Function CallRecord ● On ○ Off

Login Name rgordon
Password
Allocated Memory (%) 18
Mem Overflow Action ● Reject Calls ○ Don't Record

Messages:

```
----------------------------------------------------
Wed Jul 10 18:19:03 EDT 1996 (Retrieving information from nmsw3...)
Wed Jul 10 18:19:04 EDT 1996 (Using values retrieved from switch nmsw3 as
reference)
```

Figure 14.1 - Call Records Configuration Dialog

Use the Call Record Config dialog to configure call records and performance monitoring data for billing purposes. The parameters are defined as follows:

Primary IP Address (or URL) Identifies the primary address (or URL) for call record transfers. This includes the IP address host to contact, and optionally the port on that host, and a directory on that host to put the data.

The URL is in the following form:

`URL = //<ip-address>[:port]`
or

`URL = //<ip-address>[:port][<pathname>]/`

where **`ip-address`** indicates the IP address of the host to contact; **`port`** indicates the port on the host to contact; **`pathname`** indicates the directory on the host into which the data should be put.

NOTE: When a pathname is specified, the call record file is placed into that directory with the automatically generated file name.

Primary Filename The filename associated with the Primary IP Address, in the following format:

`FILE = [<filename>]`

When a filename is specified, the call record file uses the filename as a prefix for the final file name (prefix+automatically generated file name). The autogenerated filename contains a string of characters consisting of the following special tokens:

%T Identifies the type of switch.

%N Indicates the “SerialNumber” for a switch that has a single fabric (ASX-200, ASX-200BX, ASX-200WG) or “EnclosureNumber.SerialNumber” for a multi-fabric switch within an enclosure (ASX-1000).

%I Indicates the switch’s IP address (e.g., 169.144.1.90).

%D Indicates the date and time formatted as follows: YYMMDDhhmm.

%R Indicates the interval between recordings in minutes.

%C Identifies the contents of the call record file; **account** is for call record data and **stats** is for performance monitoring data.

%F Indicates the status of the file; **co** is for the file to which the switch fabric is currently writing, **cc** is for the file to which the switch fabric has completed writing. If the pathname is not specified, the default file is transferred to the login directory specified in <**userid**>. The following string is used as the default filename in the case where the URL ends with a " / " (i.e., without any filename):

```
%T_%C.%D.%R.%N.%F
```

If multiple switches are to write to the same location, the pathname or filename should contain either a **%I** or a **%N** token. A **%D** token in the filename portion separates each recording interval worth of data into a different file with the name being the time that the file was created. The following example would record every switch type and switch IP into a separate directory with a file at each recording interval:

```
//169.144.1.5/usr/auditlog/%T/%I/%D
```

Given an ASX-200WG switch with an IP address of 169.44.4.4, this would produce files in the following directory tree structure:

```
/usr/auditlog/ASX200-WG/169.44.4.4/
9608252355
```

If the filename specified is not made up of the above tokens, then it is used as a prefix to the default filename. If the file transfer attempt fails, the switch generates a trap and attempts a transfer to the **Secondary IP Address**. If crAdminStatus is ‘on', and this value is changed, the change goes into effect at the next aligned crXfrRecordingInterval.

Secondary IP Address (or URL) This is the specification of the Secondary URL for callrecord transfers. The URL includes the IP address host to contact, and optionally the port on that host, the directory on that host to put the data into and the filename. This URL is to be used only if the transfer to Primary URL is not successful. If the file transfer attempt to this URL also fails, the switch will generate a trap.

Secondary Filename The filename associated with the Secondary URL, containing strings of characters consisting of special tokens. Please see the description for Primary Filename for information on the tokens.

Configure Switch Time Launches the Switch Time Configuration dialog which is used to synchronize the current date and time across switches.

Function Toggled variable to select which function to enable, either **`Callrecord`**, or **`Performance`**.

Login Name Indicates the userid to be used for the data transfer sessions to the primary and secondary data servers.

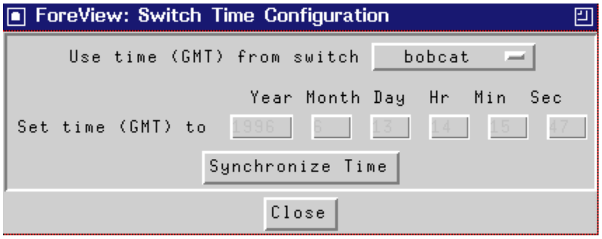
Password Indicates the password to be used for the data transfer sessions to the primary and secondary data servers.

Allocated Memory (%) Indicates a percentage specifying what portion of the processor DRAM is to be reserved for call records. The default setting is **`15%`**. Valid values are from **`10%`** to **`50%`**. Changing this value affects the amount of memory available for signalling and routing, and may result in increased call blocking. A change in this MIB value takes effect only after the next call record initialization (i.e., when the crAdminStatus changes from ‘off' to any other valid value or the switch (fabric) is rebooted).

Mem Overflow Action Indicates the action that the switch (fabric) should take if the memory allocated for call records runs out. Choosing **`Reject Calls`** means that the call should be rejected. Choosing **`Don’t  Record`** means that the call should be allowed, but no call record should be generated for that call. The default setting is **`Reject Calls`**. If this value is changed, the change takes effect immediately.

14.2.1 Synchronizing Switch Time

To synchronize the time on a switch, launch the Switch Time Configuration by clicking on the **`Configure Switch Time`** button on the Call Record Config dialog. The Switch Time Configuration dialog is used to synchronize the current date and time across switches.



ForeView: Switch Time Configuration

Use time (GMT) from switch bobcat

Set time (GMT) to Year 1996 Month 6 Day 13 Hr 14 Min 15 Sec 47

Figure 14.2 - Switching Timing Configuration Dialog

14.3 Post Processing of Records

ForeView provides two utilities to aid in the post-processing of call record and performance monitoring data. These utilities convert the call record and performance record file data from binary format to ascii format. Because most standard databases and spreadsheet programs import ascii files, information can be extracted and reports can be produced easily.

14.3.1 Record Output

The call record post-processing utility, fvcrb2a, is invoked by typing a command of the form:

```
fvcrb2a [filename...]
```

The performance record post-processing utility, fvprb2a, is invoked by typing a command of the form:

```
fvprb2a [filename]
```

Additionally, the following two arguments provide a field separator option and an output format enhancement:

-Fc For the field separator, **-Fc** specifies that the character ‘c’ be used as the field separator. The default is to use a comma as the separator.

-s For the format, **-s** specifies the format of the output into a line-by-line format for easier reading.

Field separators are, by default, commas. This can be restricting if the text of a field contains commas. Thus you can redefine the field separator with the **-Fc** argument and then process the file as required.

NOTE

The following characters, “.”, “()”, and the space are reserved and cannot be used as field separators.

For most purposes, these utilities will handle the input as part of a default action which is to scan (read) the input data line by line. In the event that formatted output is desired, the **-s** argument must be used. For both the above arguments, output will be to the terminal.

For example, to modify the field separator and output of a call record file, the command must be modified as follows:

```
fvcrb2a -Fc [filename...]
```

14.3.2 Call Record Data

The output format for the call record post-processing untility (fvcrb2a) is as follows:

Line Number	Contents
1	File name.
2 to 11	File header information.
12	A comprehensive list of the fields contained in the call record, including call record type, call connection identifier, call connection point, etc.
13 to n	The values for each call record field. If the value of any field is missing, ## is inserted in place of the value.

14.3.3 Performance Record Data

The output format for the performance record post-processing untility (fvprb2a) is as follows:

Line Number	Contents
1	File name
2 to 11	File header information
12	Netmod data field description
13	Port shared memory priority data
14	Port shared memory priority data field description
15	DS1 port record header
16	DS1 port record field description
17	DS3 port record header
18	DS3 port record field description
19	OC3 port record header
20	OC3 port record field description
21	OC12 port record header
22	OC12 port record field description
23	E1 port record header

24 E1 port record field description

25 E3 port record header

26 E3 port record field description

27 J2 port record header

28 J2 port record field description

29 to n Headers identified above plus the associated valued for each performance record type.

14.4 Call Record and Performance Record Statistics

14.4.1 Call Record Statistics

The call record data collection application supports call record generation for calls established configured via PVCs, PVPs, and SPVCs under SPANS PNNI, or through UNI 3.x signalling SVCs. Call records are generated for user connections only. The call record contents are defined in the following table.

Field	Description
call_conn_id	32-byte identifier
call_orig_method	crm_orig_pp (point-to-point) crm_orig_pmp (point-to-multipoint) crm_orig_mpp (multipoint-to-point) crm_orig_mpmp (multipoint-to-multipoint)
call_type	crm_pvc crm_pvp crm_q2931_svc crm_pnni_spvc
call_start_time	ISO 8601 format CCYYYYMMDDThhmmss.s
call_collect_time	ISO 8601 format CCYYYYMMDDThhmmss.s
call_in_port_vp_vc	Input port name, VPI, VCI string
call_status	crm_call_setup crm_call_new crm_call_inprogress crm_call_setup_term crm_call_new_n_term crm_call_inprog_term
call_carrier_id	
call_interface_id	
call_nsap_calling	NSAP address of the originating end point of the call
call_nsap_called	NSAP address of the remote end point of the call
call_nsap_sub_called	
call_cell_recvd	Cumulative count of the receieved cells
call_cell_rejected	Cumulative count of the rejected cells

call_cell_xmitd Cumulative count of the transmitted cells

call_forw_pcr_clp_0 The peak cell rate for all forward cells

call_forw_pcr_clp_01 The peak cell rate for forward cells with CLP = 0

call_back_pcr_clp_0 The peak cell rate for all backward cells

call_back_pcr_clp_01 The peak cell rate for backward cells with CLP = 0

call_forw_scr_clp_0 The sustainable cell rate for forward cells with CLP = 0

call_forw_scr_clp_01 The sustainable cell rate for all forward cells

call_back_scr_clp_0 The sustainable cell rate for backward cells with CLP = 0

call_back_scr_clp_01 The sustainable cell rate for all backward cells

call_forw_mbs_clp_0 The maximum burst size for forward cells with CLP = 0

call_forw_mbs_clp_01 The maximum burst size for all forward cells

call_back_mbs_clp_0 The maximum burst size for backward cells with CLP = 0

call_back_mbs_clp_01 The maximum burst size for all backward cells

call_forw_qos ATM Forum UNI Definition

call_back_qos ATM Forum UNI Definition

call_count_validity_flg Indicates the validity of the cell count

call_record_type crm_pvp_pvc
crm_svc
crm_spvc

call_in_connect_point crm_conn_pt_orig
crm_conn_pt_tran
crm_conn_pt_term

call_term_cause_value

call_spvc_assoc_pvc_id call_traffic_mgmt
call_best_effort
call_spans_calling
call_spans_called

call_out_port_vp_vc	
call_out_connect_point	crm_conn_pt_orig crm_conn_pt_tran crm_conn_pt_term
call_traffic_mgmt	The management action for traffic. **Tag** means that non-compliant CLP = 0 cells are tagged. **Drop** means that non-compliant cells are dropped.
call_best_effort	
call_spans_calling	
call_spans_called	
call_recv_count_offset	
call_user_orig_method	crm_orig_pp crm_orig_pmp crm_orig_mpp crm_orig_mpmp

14.4.2 Performance Record Statistics

Type of Record	Data Elements
Board Data	Board id, vpiLookupErrors, vciLookupErrors
Network Module	Network module id, uptime
Shared Memory	Port id in bnp format, queue sizes, transmitted cells, lost cells
DS-1	Port id in bnp format, buffer size, queue length, overflows, hardware errors, number of paths in/out, maximum bandwidth in/out, received cells, transmitted cells, framing errors, plcp errors, ATM header check sequence errors
DS-3	Port id in bnp format, buffer size, queue length, overflows, hardware errors, number of paths in/out, maximum bandwidth in/out, received cells, transmitted cells, framing errors, plcp errors, ATM header check sequence errors

OC-3 Port id in bnp format, buffer size, queue length, overflows, hardware errors, number of paths in/out, maximum bandwidth in/out, received cells, transmitted cells, section errors, line errors, path errors, ATM correctable/uncorrectable header check sequence errors

OC-12 Port id in bnp format, buffer size, queue length, overflows, hardware errors, number of paths in/out, maximum bandwidth in/out, received cells, transmitted cells, section errors, line errors, path errors, ATM correctable/uncorrectable header check sequence errors

E-1 Port id in bnp format, buffer size, queue length, overflows, hardware errors, number of paths in/out, maximum bandwidth in/out, received cells, transmitted cells, framing errors, plcp errors, ATM header check sequence errors

E-3 Port id in bnp format, buffer size, queue length, overflows, hardware errors, number of paths in/out, maximum bandwidth in/out, received cells, transmitted cells, framing errors, plcp errors, ATM header check sequence errors

J-2 Port id in bnp format, buffer size, queue length, overflows, hardware errors, number of paths in/out, maximum bandwidth in/out, received cells, transmitted cells, coding errors, crc5 errors, ATM header check sequence errors

14.5 Example Application

This section illustrates the necessary steps to set up the Call Record Config dialog to facilitate the data collection and file transfer of call records and performance records.

1. Launch the Call Record Config dialog.
2. Add the names of the switch or switches from which you want to generate records.
3. Fill in the **`Primary URL`** and **`Primary Filename`** entries.

NOTE

Enter a **`Secondary URL`** and a **`Secondary Filename`** as a backup should access to the primary URL fail.

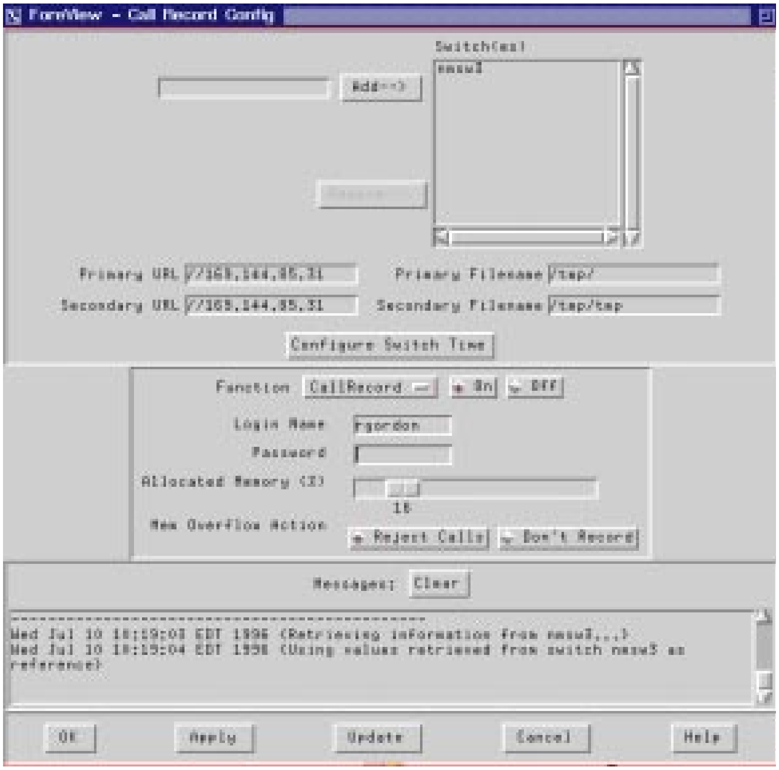
4. Select the desired function by toggling to either **`CallRecord`** or **`Performance`**.
5. Click the **`On`** button to enable the function.
6. Enter a valid **`Login Name`** and **`Password`**.

NOTE

For call records, select values for **`Allocated Memory`** and **`Mem Overflow Action`**. The default setting for **`Allocated Memory`** is **`15%`**. The default setting for **`Mem Overflow Action`** is **`Reject Calls`**. These options are not valid for performance records.

7. Click on the **`Apply`** button to initiate data collection.

The following figure illustrates a call record setup.



Switch(es): nmsw3

Primary URL //169.144.85.31 Primary Filename /tmp/

Secondary URL //169.144.85.31 Secondary Filename /tmp/tmp

Function CallRecord ● On ○ Off

Login Name fgordon

Password

Allocated Memory (%) 18

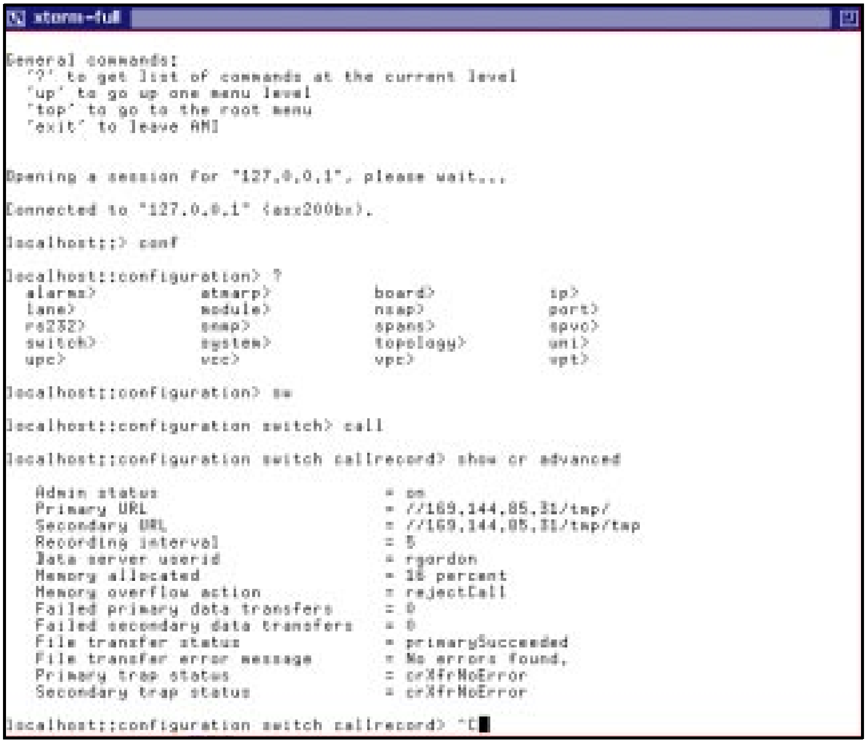
Mem Overflow Action ● Reject Calls ○ Don't Record

Messages:

```
--------------------------------------------
Wed Jul 10 18:19:03 EDT 1996 (Retrieving information from nmsw3...)
Wed Jul 10 18:19:04 EDT 1996 (Using values retrieved from switch nmsw3 as
reference)
```

Figure 14.3 - Call Record Configuration

To verify whether the file transfer was successful, log into the switch to view the call record status. The following figure shows the call records statistics. Note the **`primarySucceeded`** value next to the **`File transfer status`** entry. This denotes the successful transfer of call record data.

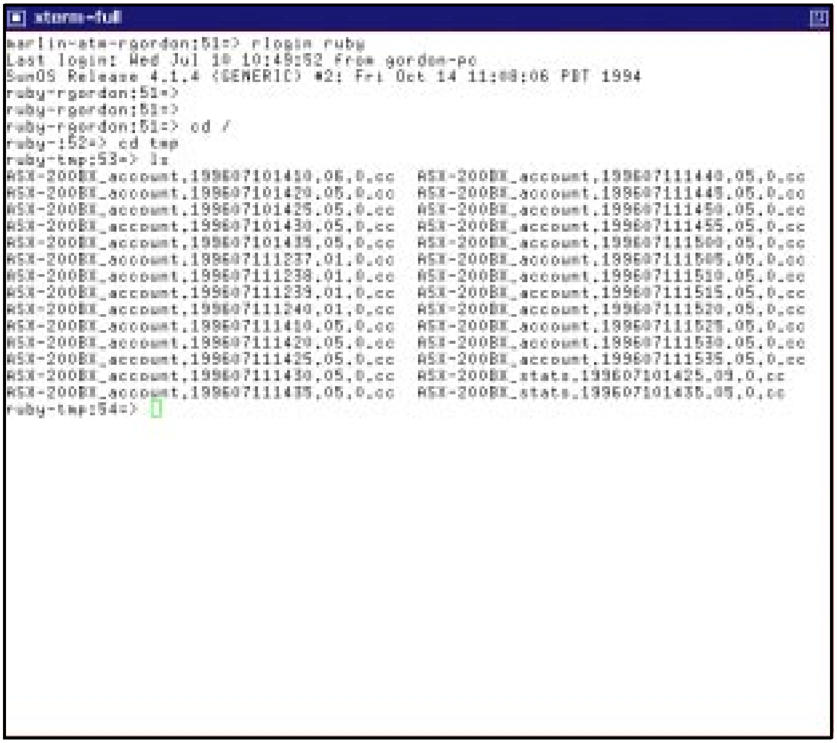


```
General commands:
  '?' to get list of commands at the current level
  'up' to go up one menu level
  'top' to go to the root menu
  'exit' to leave AMI


Opening a session for "127.0.0.1", please wait...

Connected to "127.0.0.1" (asx200bx).

localhost::> conf

localhost::configuration> ?
  alarms>            atmarp>            board>             ip>
  lane>              module>            nsap>              port>
  rs232>             snmp>              spans>             spvc>
  switch>            system>            topology>          uni>
  upc>               vcc>               vpc>               vpt>

localhost::configuration> sw

localhost::configuration switch> call

localhost::configuration switch callrecord> show or advanced

   Admin status                         = on
   Primary URL                          = //169.144.85.31/tmp/
   Secondary URL                        = //169.144.85.31/tmp/tmp
   Recording interval                   = 5
   Data server userid                   = rgordon
   Memory allocated                     = 16 percent
   Memory overflow action               = rejectCall
   Failed primary data transfers        = 0
   Failed secondary data transfers      = 0
   File transfer status                 = primarySucceeded
   File transfer error message          = No errors found.
   Primary trap status                  = crXfrNoError
   Secondary trap status                = crXfrNoError

localhost::configuration switch callrecord> ^C
```

Figure 14.4 - Call Record Verification

14.5.1 Post Processing of Records

To view the files transferred to the primary URL, log into the host to view the records. The following figure shows the records that were generated in the previous example. Note the files with **`_account`** in the prefix are call records. Files with **`_stats`** in the prefix are performance records.



```
merlin-atm-rgordon:51=> rlogin ruby
Last login: Wed Jul 10 10:49:52 from gordon-pc
SunOS Release 4.1.4 (GENERIC) #2: Fri Oct 14 11:08:06 PDT 1994
ruby-rgordon:51=>
ruby-rgordon:51=>
ruby-rgordon:51=> cd /
ruby-:52=> cd tmp
ruby-tmp:53=> ls
ASX-200BX_account.199607101410.05.0.cc  ASX-200BX_account.199607111440.05.0.cc
ASX-200BX_account.199607101420.05.0.cc  ASX-200BX_account.199607111445.05.0.cc
ASX-200BX_account.199607101425.05.0.cc  ASX-200BX_account.199607111450.05.0.cc
ASX-200BX_account.199607101430.05.0.cc  ASX-200BX_account.199607111455.05.0.cc
ASX-200BX_account.199607101435.05.0.cc  ASX-200BX_account.199607111500.05.0.cc
ASX-200BX_account.199607111237.01.0.cc  ASX-200BX_account.199607111505.05.0.cc
ASX-200BX_account.199607111238.01.0.cc  ASX-200BX_account.199607111510.05.0.cc
ASX-200BX_account.199607111239.01.0.cc  ASX-200BX_account.199607111515.05.0.cc
ASX-200BX_account.199607111240.01.0.cc  ASX-200BX_account.199607111520.05.0.cc
ASX-200BX_account.199607111410.05.0.cc  ASX-200BX_account.199607111525.05.0.cc
ASX-200BX_account.199607111420.05.0.cc  ASX-200BX_account.199607111530.05.0.cc
ASX-200BX_account.199607111425.05.0.cc  ASX-200BX_account.199607111535.05.0.cc
ASX-200BX_account.199607111430.05.0.cc  ASX-200BX_stats.199607101425.05.0.cc
ASX-200BX_account.199607111435.05.0.cc  ASX-200BX_stats.199607101435.05.0.cc
ruby-tmp:54=> 
```

Figure 14.5 - Records Transfer Verification

Use the call record post-processing utility to convert a call record file data from binary format to ascii format. The call record post-processing utility, fvcrb2a, is invoked by typing a command of the form:

```
fvcrb2a [filename...]
```

In the event that formatted output is desired, the **-s** argument must be used. For example, to format the output of a call record file from the example, the command would be entered as follows:

```
fvcrb2a -s /tmp/ASX-200BX_account.199607111440.05.0.cc
```

14.6 Call Records from the Command-line

For convenience, *ForeView*'s Call Records utility can be run from the command-line of your operating system. The following explains the command-line syntax:

fvcall *[-cw write_community] [-cr read_community] [switch...]*

where *switch* is the IP hostname or ATM address of a switch in a ForeRunner ATM network.

CHAPTER 15 Software Manager

This feature requires *ForeThought* software version 4.1.0 or greater to be running on your switches.

ForeView provides a utility to facilitate upgrades of the software running on FORE ATM switches. Before beginning the upgrade process, you will need the upgrade file from FORE Systems. This file can be obtained via ftp or diskette. To obtain the file via ftp, you must have ftp access. To obtain the file from diskette, you will need the distribution diskettes from FORE Systems.

NOTE

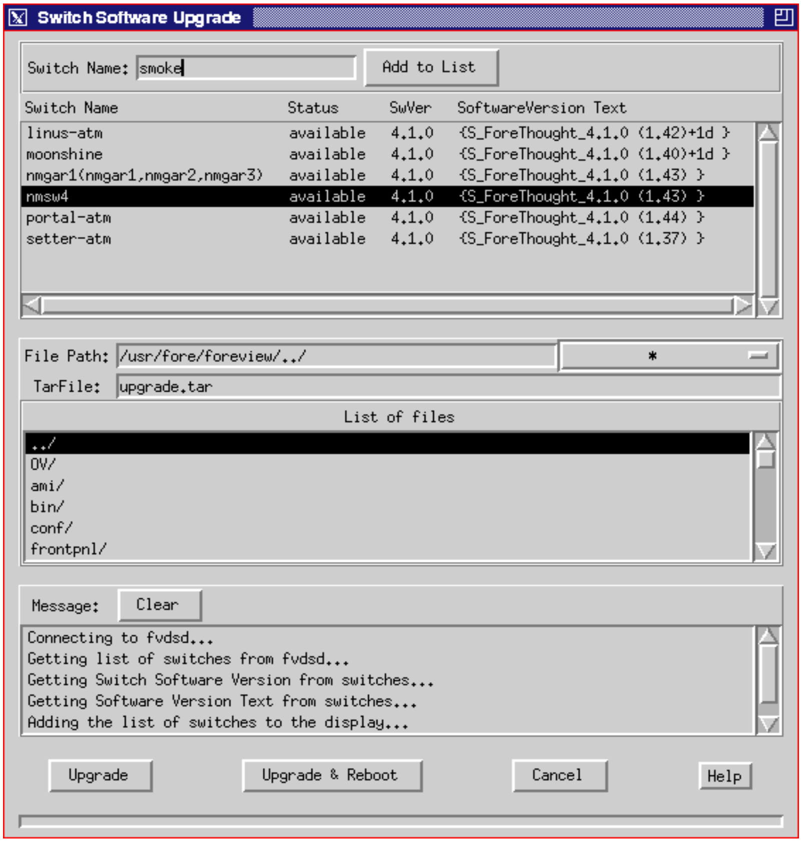
There are instructions for obtaining the upgrade file in the *ForeRunner* ATM Switch User's Manual. This chapter also contains upgrade requirements that are specific to the ASX-1000, ASX-200WG, and the ASX-200.

To start the Software Manager, type the following command at the shell prompt:

```
fvswmgr
```

If no hostnames are passed on the command line, the Software Manager discovers all the switches in the ATM network whose current software version supports a software-based upgrade (i.e. *ForeThought* 4.1.0 or higher).

The display shows the switches available for upgrade, the current version of the software that each one is running, and the current status of each switch, as shown in the following figure.



Switch Name: smoke

Switch Name	Status	SwVer	SoftwareVersion Text
linus-atm	available	4.1.0	{S_ForeThought_4.1.0 (1.42)+1d }
moonshine	available	4.1.0	{S_ForeThought_4.1.0 (1.40)+1d }
nmgar1(nmgar1,nmgar2,nmgar3)	available	4.1.0	{S_ForeThought_4.1.0 (1.43) }
nmsw4	available	4.1.0	{S_ForeThought_4.1.0 (1.43) }
portal-atm	available	4.1.0	{S_ForeThought_4.1.0 (1.44) }
setter-atm	available	4.1.0	{S_ForeThought_4.1.0 (1.37) }

File Path: /usr/fore/foreview/../ *

TarFile: upgrade.tar

List of files

```
../
OV/
ami/
bin/
conf/
frontpnl/
```

Message:

```
Connecting to fvdsd...
Getting list of switches from fvdsd...
Getting Switch Software Version from switches...
Getting Software Version Text from switches...
Adding the list of switches to the display...
```

Figure 15.1 - Software Manager Utility

You may choose one or more of the available switches, and select the appropriate file (which is expected to be a tar file containing the new switch software).

The following options are available using the Software Manager:

Upgrade Select Upgrade to transfer the tar file to the switch or switches selected for software upgrades.

NOTE: The switch will continue to run the old software until reboot.

Upgrade & Reboot Select Upgrade & Reboot to transfer the tar file to the switch or switches selected for software upgrades. The switches undergo a warmstart when rebooted.

NOTE: This may result in a loss of the existing Virtual Channels and Paths. See Chapter 5 of the *ForeRunner* ATM Switch User's Manual for precautions to take before upgrading switch software.

Cancel Select Cancel to exit the Software Manager before any switches are upgraded.

Help Select Help to view the contents of the help file for the Software Manager.

NOTE

Reminder. The upgrade utility is supported only by *ForeThought* software versions 4.1.0 and greater.

15.1 Software Upgrades from the Command-line

For convenience, *ForeView*’s Software Manager utility can be run from the command-line of your operating system. The following explains the command-line syntax:

fvupgrad *[-cw write_community] [-cr read_community] [hostname ...]*

If no hostnames are passed on the command-line, fvupgrad discovers all the switches in the ATM network whose current software version supports a software based upgrade (i.e. *ForeThought* version 4.1.0 or higher).

CHAPTER 16 Remote Console Interface and Scripting with AMI

16.1 What Is AMI?

This chapter serves as an introduction to the ATM Management Interface (AMI) system. AMI provides a hierarchical menu system similar to a UNIX file system. There is a single root menu which provides a number of commands. Some of those commands call submenus which provide a number of subcommands.

AMI can be run on any *ForeRunner* switch running version 3.0.1 or later switch software. It is also available with *ForeView* and can be used as a scripting language to build utilities. At any given time, you can work within a particular submenu which is indicated by the specific prompt for that level. You can traverse each level of a submenu one level at a time, or traverse a number of levels simultaneously if the entire command string is known. For example, to show the current configuration of the network modules, type the following at the prompt:

```
localhost::> configuration module show
```

rather than typing one command line at a time as follows:

```
localhost::> configuration

localhost::configuration> module

localhost::configuration module> show
```

Additionally, you only need to enter the minimum number of letters in a command which would make the command unique to that level. For example, you could enter **co m s** instead of **configuration module show**. However, the minimum number of letters entered must also distinguish the command from global commands, such as **up**. For example, you would have to enter **upc** to distinguish **upc** from the global command **up**.

AMI uses the following conventions:

- Commands that contain submenus are immediately followed by a “>” symbol. The “>” should not be entered as part of the command.
- Required parameter values are indicated inside angle brackets “<>”. The “<>” should not be entered as part of the command.
- Optional parameter values are indicated inside square brackets “[]”. The “[]” should not be entered as part of the command.
- Parameter value choices are separated by vertical bars “ | ”.
- Optional parameter names are indicated with dashes “-”.
- All port numbers are in BNP (board-network module-port) notation.

16.1.1 Where to Find More Information on AMI

All AMI commands are documented in the current ATM Management Interface (AMI) Manual. Contact FORE Systems’ Technical Support for more information. Refer to the Preface of this manual for information on how to contact Technical Support.

16.2 Initial Login from Serial Port or Telnet

You can log into the switch either through the serial port or through the Ethernet port using telnet.

16.2.1 Login from Serial Port

When connecting to the switch via the serial port, output similar to the following will be displayed on your console:

```
ForeThought_4.0.0 (1.15) (asx200bx) (fishtank)
```

Above, **`ForeThought_4.0.0 (1.15)`** indicates the version of software, **`(asx200bx)`** indicates what type of switch this is, and **`(fishtank)`** indicates the name that has been assigned to this SCP. If **`(ATM SWITCH)`** is displayed for the switch name, this means that no host name has been assigned yet.

At the login prompt, if a password has been assigned to the switch, you should type **`asx <ENTER>`** and then type the password. The switch will not echo the keystrokes of the password for security reasons.

```
login: asx
Password:
```

If no password has been assigned, enter **`asx <ENTER>`** at the serial port. In either case, the following is displayed and a session is opened on the SCP:

```
ATM Management Interface v1.2
Copyright (c) 1994, 1995 FORE Systems, Inc.
All Rights Reserved

General commands:
  '?' to get list of commands at the current level
  'up' to go up one menu level
  'top' to go to the root menu
  'exit' to leave AMI

Opening a session for “127.0.0.1”, please wait...

Connected to “127.0.0.1” (asx200bx).
```

Remote Console Interface and

```
localhost::>
```

16.2.2 Login from Telnet

To telnet to the SCP, enter the following parameters at the > prompt on the host:

```
> telnet <name>
```

name Enter either the name or the IP address of the SCP.

For example, to telnet to an SCP called fishtank, enter the following:

```
> telnet fishtank
```

When the telnet connection is established, something similar to the following will be displayed:

```
Trying 204.95.89.231 ...
Connected to fishtank.
Escape character is '^]'.

ForeThought_4.0.0 (1.15) (asx200bx) (fishtank)
```

Above, **`ForeThought_4.0.0 (1.15)`** indicates the version of software, **`(asx200bx)`** indicates what type of switch this is, and **`(fishtank)`** indicates the name that has been assigned to this SCP. If **`(ATM SWITCH)`** is displayed for the switch name, this means that no host name has been assigned yet.

Only one user may open an AMI session on an SCP at a time. You will be prompted to log in. You should enter **`ami`** at the prompt.

NOTE

On an ASX-200, log in as **`asx`**. More than one user may log in to an ASX-200 at one time.

If a password has been assigned, then you will be prompted for that password. The keystrokes of the password will not be echoed for security reasons. If no password has been assigned (e.g., the very first time you log in), then you will not be prompted for a password.

```
login: ami
Password:
```

The following is displayed and a session is opened on the SCP:

```
ATM Management Interface v1.2
Copyright (c) 1994, 1995 FORE Systems, Inc.
All Rights Reserved


General commands:
  '?' to get list of commands at the current level
  'up' to go up one menu level
  'top' to go to the root menu
  'exit' to leave AMI


Opening a session for “127.0.0.1”, please wait...

Connected to “127.0.0.1” (asx200bx).

localhost::>
```

If another user already has an AMI session open on that SCP, then you will not be permitted to log in and will receive the following message:

```
Another ami is running on this switch. . Exiting...
Connection closed by foreign host.
```

16.3 AMI Commands Not Available When Running Remotely

Some AMI commands are not available when you telnet or log in to a switch remotely. For example, if you are logged in locally to a switch called fishtank (you will see `localhost::>` as your prompt) and you open a session to a switch called shark (you will see `shark::>` as your prompt), there are some AMI commands that will not work on shark.

The following is a list of the commands that are not available when running a remote AMI session, and the applicable switch platforms.

The following commands are not available remotely on an ASX-1000:

- configuration system syslog
- configuration system timeout
- operation cdb init
- operation flash copy
- operation flash delete
- operation flash dir
- operation flash delete
- operation flash free
- operation flash init
- operation flash rename
- operation panic
- operation reboot
- operation version

The following commands are not available remotely on an ASX-200BX nor are they available remotely on an ASX-200WG that has a 16 MB SCP:

- configuration system syslog
- configuration system timeout
- operation cdb init
- operation flash copy
- operation flash delete
- operation flash dir
- operation flash delete
- operation flash free

- operation flash init
- operation flash rename
- operation panic
- operation reboot
- operation version

The following commands are not available remotely on a *ForeRunnerLE* 155:

- configuration system syslog
- configuration system timeout
- operation cdb init
- operation flash copy
- operation flash delete
- operation flash dir
- operation flash delete
- operation flash free
- operation flash init
- operation flash rename
- operation panic
- operation reboot
- operation version

16.4 PNNI Topology Configuration Commands

These commands allow you to manage the *ForeThought* PNNI topology information and the SPANS topology information of the switch fabric. You can display the list of available subcommands by typing **`topology ?`** at the **`configuration`** level.

```
localhost::configuration> topology ?
  forepnni>        spans>
```

16.4.1 *ForeThought* PNNI Configuration Commands

These commands allow you to modify various aspects of *ForeThought* PNNI on a switch. You can display the list of available subcommands by typing **`forepnni ?`** at the **`topology`** level.

```
localhost::configuration topology> forepnni ?
  prefix           border           swmask           pgmask
  hello            nsapindication   staticupdate     maxhop
  propmult         minthresh        vcmark           show
```

16.4.1.1 Setting the *ForeThought* PNNI Switch Prefix

When using *ForeThought* PNNI, a switch fabric is identified by a variable length NSAP switch prefix which ranges in length from 0 to 13 bytes. This command allows you to set the *ForeThought* PNNI prefix on the switch. Enter the following parameters:

```
localhost::configuration topology forepnni> prefix <prefix>
```

prefix Indicates the default NSAP prefix for this ATM switch that is used in the ILMI address registration message and in the hello indication SPANS-NNI message.

NOTE The switch software must be restarted for this command to take effect. Therefore, you must be in a local AMI session to perform this command.

16.4.1.2 Changing the *ForeThought* PNNI Border Switch Functionality

A switch that has a link to another switch that belonging to a different peergroup is considered a border switch. A border switch advertises reachability to its peergroup to switches outside of its peergroup, but it does not share its peergroup's topology with the other switches. You should enable border switch functionality on all switches that are on the outside edges of all of the peergroups that you have established. This command lets you designate whether or not this switch will act as a *ForeThought* PNNI border switch. Enter the following parameters:

```
localhost::configuration topology forepnni> border (enable | disable)
```

enable|disable Entering **enable** (and rebooting) means that this switch will act as a *ForeThought* PNNI border switch. Entering **disable** (and rebooting) means that this switch will not act as a *ForeThought* PNNI border switch.

NOTE The switch software must be restarted for this command to take effect. Therefore, you must be in a local AMI session to perform this command.

16.4.1.3 Setting the *ForeThought* PNNI Switch Prefix Mask

This command allows you to select the *ForeThought* PNNI switch prefix mask value. Enter the following parameters:

```
localhost::configuration topology forepnni> swmask <mask>
```

mask Indicates the mask that gives the number of leading bits in the switch prefix used to aggregate the addresses that belong to the switch in *ForeThought* PNNI. The default switch prefix mask value is 104.

NOTE The switch software must be restarted for this command to take effect. Therefore, you must be in a local AMI session to perform this command.

16.4.1.4 Setting the *ForeThought* PNNI Peergroup Mask

A peergroup mask is the length (in the number of bits) of the peergroup ID of a switch. This command enables you to set the *ForeThought* PNNI peergroup mask value. This value should be the same for all members of a peergroup. Enter the following parameters:

```
localhost::configuration topology forepnni> pgmask <mask>
```

mask Indicates the mask that gives the number of leading bits in the switch prefix used to aggregate the addresses that belong to this *ForeThought* PNNI peergroup. The default peergroup mask value is 0.

NOTE The switch software must be restarted for this command to take effect. Therefore, you must be in a local AMI session to perform this command.

16.4.1.5 Setting the Hello Indication Interval

Hello indication messages are the "keep alive" messages that two switches send to one another to verify their existence. This command lets you change the interval for *ForeThought* PNNI hello indication messages. Enter the following parameters:

```
localhost::configuration topology forepnni> hello <msec>
```

msec Indicates the period of time, in milliseconds, between transmissions of hello indication messages. The default value is **`500`** milliseconds.

16.4.1.6 Setting the NSAP Indication Interval

NSAP indication messages are those messages that update topology information between any two switches. This command allows you to select the interval for *ForeThought* PNNI NSAP indication messages. Enter the following parameters:

```
localhost::configuration topology forepnni> nsapindication <msec>
```

msec Indicates the period of time, in milliseconds, between transmissions of NSAP indication messages. The default value is **`10,000`** milliseconds.

16.4.1.7 Setting the Static Route Update Indication Interval

Static route update indication messages are refresh messages that update topology information about static routes. This command enables you to set the interval for *ForeThought* PNNI static route indication messages. Enter the following parameters:

```
localhost::configuration topology forepnni> staticupdate <msec>
```

msec Indicates the period of time, in milliseconds, between transmissions of static route update indication messages. The default value is **10,000** milliseconds.

16.4.1.8 Setting the Maximum Hop Count

By setting a maximum hop count, you tell the switch to consider only those paths that have less than or equal to the number of hops specified when setting up a connection. If a connection is routed using a path with a large hop count, there is a greater chance that the connection may experience congestion and be delayed or discarded. This command lets you set the maximum hop count for the NSAP router. Enter the following parameters:

```
localhost::configuration topology forepnni> maxhop <hops>
```

hops Indicates the maximum number of hops to use when routing a connection for the NSAP router. The default value is **20** hops.

16.4.1.9 Setting the Proportional Multiplier

This command enables you to set the proportional multiplier for the NSAP router. The proportional multiplier is expressed as a percentage of Available Cell Rate (ACR) on any given link in the network. If the change in percentage of the ACR on any given link in the NSAP topology of the network exceeds this percentage threshold, then the change is considered significant. The topology tables are then updated accordingly for that link. Enter the following parameters:

```
localhost::configuration topology forepnni> propmult <percentage>
```

percentage Indicates the threshold, entered as a percentage, above which you consider the change in ACR on any link to be significant. The default value is **20**%.

NOTE If you modify this value, you should modify it on all switches in the network.

16.4.1.10 Setting a Minimum Threshold for NSAP Updates

The minimum threshold is the smallest capacity value that the threshold value for determining the significant change in ACR can take. This minimum value ensures that the threshold value does not become a very small value in cases in which product of the ACR and the proportional multiplier is a very small number. The minimum threshold is used to prevent excessively frequent NSAP updates resulting from minor changes in ACR when the value of ACR is very low. Enter the following parameters:

```
localhost::configuration topology forepnni> minthresh <minthresh>
```

minthresh Indicates the minimum threshold bandwidth value for triggering NSAP updates, entered in kilobits per second. The default value is **50** kilobits per second.

16.4.1.11 Setting a Minimum Virtual Channel Mark

When the number of available virtual channels on a path drops to zero, a link state update is sent out to advertise that there are no more VCs available for use on this path. When the number of VCs indicated by the **vcmark** is available for use on this path again, another link state update is sent out to advertise that there are VCs available for use on this path once again. This command lets you set the **vcmark**, which is the minimum number of virtual channels that need to be to available on a path to make that path usable again. Enter the following parameters:

```
localhost::configuration topology forepnni> vcmark <vcmark>
```

vcmark Indicates the minimum number of virtual channels that need to be to available on a path to make that path usable. The default value is **20** VCs.

16.4.1.12 Displaying *ForeThought* PNNI Parameters

This command lets you display all of the *ForeThought* PNNI topology parameters. Enter the following parameters:

```
localhost::configuration topology forepnni> show

Switch NSAP prefix                    0x47.0005.80.ffe100.0000.f215.0df6
Switch Prefix Mask                       104
Peer Group Mask                          0

Hello Indication Interval                500 msec
NSAP Indication Interval                 10000 msec
Static Route Update Interval             10000 msec
Max hop count for NSAP router            20 hops
Proportional Multiplier                  20 %
Minumum Threshold for NSAP updates       50 Kbps
Minimum VC level                         20

FORE PNNI border switch functionality is disabled
```

The fields in this display are defined as follows:

Switch NSAP prefix Displays the switch’s NSAP prefix.

Switch Prefix Mask Shows the switch prefix mask value of high-order bits to use for aggregating addresses on the switch for routing purposes.

Peer Group Mask Lists the peergroup mask value of high-order bits to use for aggregating addresses on the switch for routing purposes.

Hello Indication Interval Displays the period of time between transmissions of hello indication messages, in milliseconds.

NSAP Indication Interval Shows the period of time between transmissions of NSAP indication messages, in milliseconds.

Static Route Update Interval Lists the period of time between transmissions of static route update indication messages, in milliseconds.

Max hop count for NSAP router Displays the maximum number of hops to use when routing a connection for the NSAP router.

Proportional Multiplier Shows the threshold, in percentage, above which the change in ACR on any link is considered to be significant.

Minimum Threshold for NSAP updates Lists the minimum threshold bandwidth value for triggering NSAP updates, in kilobits per second.

Minimum VC level Lists the minimum number of VCs that need to be available on a path to make that path usable again after the number of available VCs has dropped to zero.

FORE PNNI border switch functionality is disabled If this functionality is **enabled**, this switch acts as a *ForeThought* PNNI border switch. If this functionality is **disabled**, this switch does not act as a *ForeThought* PNNI border switch.

16.4.2 Topology Scripts

ForeView provides two scripts to set switch topology. The scripts, **set_pnni** and **set_spans**, run under OpenView and call **snmpset** in **/usr/OV/bin/**.

16.4.2.1 PNNI Topology Script

The following script in set_pnni.tcl can be used to set PNNI information for a switch or switches. The user-defined parameters are identified by the comment marks (#). For multiple switches, put a space between each corresponding parameter entry.

For example, multiple switches would be defined as follows:

```
set switches {nmsw2 nmsw3 labswitch1 }
```

Next, the write community parameter for each switches would be defined as follows:

```
set community {private private public }
```

Follow this format for all of the user-defined parameters. Make sure there is a one-to-one correlation between switches and topology parameters.

```
#define switches
set switches {nmsw2  }

#set write community for switches
set community {private}

#define switch prefixes
set prefixes {0x47.0005.80.ffe100.0000.f215.122d}

#define switch prefix masks
set swmasks {104}

#define peer group mask here
set pgmasks {0}

#define Hello Indication Interval(msec)
set hellos {400}

#define NSAP Indication Interval (msec)
```

```
set indications {10000}

#define Static Route Update Interval(msec)
set route {1000}

#define max hops here
set maxhops {20}

#define Proportional Multiplier(percentage)
set multiplier {20}

#define Minumum Threshold for NSAP updates
set threshold {50}

#define boarder enable here
set borders {enable}
```

16.4.2.2 SPANS Topology Script

The following script in set_spans.tcl can be used to set SPANS information for a switch or switches. The user-defined parameters are identified by the comment marks (#). For multiple switches, put a space between each corresponding parameter entry.

For example, multiple switches would be defined as follows:

```
set switches {nmsw2 nmsw3 labswitch1 }
```

Next, the write community parameter for each switches would be defined as follows:

```
set community {private private public }
```

Follow this format for all of the user-defined parameters. Make sure there is a one-to-one correlation between switches and topology parameters.

```
#define switches
set switches {nmsw2 nmsw3}

#set write community for switches
set community {private public}

#define boarder enable here
set borders {enable disabled}

#define area id here
set areas {242 837443}
```

16.5 Example Scripts

You can write a script to access AMI, allowing you to configure and to make statistical queries of various hardware and software aspects of *ForeRunner* switches and network modules.

These first two examples could be run directly from AMI. They are presented here to show examples of commands that can be embedded into `.bat` files or command scripts.

The following sections show examples of UNIX commands and a perl script that access the AMI.

16.5.1 Retrieving Switch Information

The following is a simple one line command that gives you information on a *ForeRunner* ATM switch, in this example, switch weasel:

```
echo "conf switch show" | ami weasel
```

The result looks like this:

```
ATM Management Interface v1.0
Copyright (c) 1994, 1995 FORE Systems, Inc.
All Rights Reserved
General commands:
  '?' to get list of commands at the current level
  'up' to go up one menu level
  'top' to go to the root menu
  'exit' to leave AMI

Opening a session for "weasel", please wait...

Connected to "weasel" (asx200).

weasel::>
Switch 'weasel', Type asx200
Hardware version 1.0, Software version ForeThought_3.2.0 (1.29)

Maximum Virtual Path Connections32768
Maximum Virtual Channels16384
CDVT                    1000
Policing tag
Prefix   0x47.0005.80.ffe100.0000.f215.0ce5
weasel::>
```

16.5.2 Creating a PVC

The following is a simple example of how to show all of the channels on a *ForeRunner* switch, and then create a PVC. In this example, the switch name is Panda.

First, to view the PVCs on switch Panda:

```
echo "conf vcc show" | ami panda
```

Output:

```
 ATM Management Interface v1.0
 Copyright (c) 1994, 1995 FORE Systems, Inc.
 All Rights Reserved
 General commands:
   '?' to get list of commands at the current level
   'up' to go up one menu level
   'top' to go to the root menu
   'exit' to leave AMI
 Opening a session for "panda", please wait...

 Connected to "panda" (asx100).

 panda::>
  Input          Output
Port  VPI   VCI Port  VPI   VCI Uptime        BW  Cells      CDVT Policing
  0A0     0    5 0CTL    0   34 6d:23:57       0      0       N/A N/A
  0A0     0   14 0CTL    0   33 6d:23:57       0     1M       N/A N/A
  0A0     0   15 0CTL    0   32 6d:23:57       0     9M       N/A N/A
  0A0     0   16 0CTL    0   59 6d:23:57       0 420774       N/A N/A
  0A0     0   58 0C1     0   89 0d:01:56       1 596850       N/A N/A
  0A0     0  200 0A1     0  200 6d:23:57      40      0       N/A N/A
  0A0    10  250 0A1    10  250 0d:00:27       0      0       N/A N/A
  0A0    10  250 0A2    10  250 0d:00:27       0      0       N/A N/A
  (output truncated...)
 panda::>
```

Second, create a PVC (note that you have to include the "write" community name of “private”):

```
echo "conf vcc new a0 0 110 a1 0 110" | ami panda private
```

Output:

```
ATM Management Interface v1.0
Copyright (c) 1994, 1995 FORE Systems, Inc.
All Rights Reserved
General commands:
   '?' to get list of commands at the current level
   'up' to go up one menu level
   'top' to go to the root menu
   'exit' to leave AMI
Opening a session for "panda", please wait...

Connected to "panda" (asx100).

panda::>
panda::>
```

NOTE

There is no positive confirmation that the PVC was created. However, there would be an error message if some thing went wrong.

16.5.3 Creating a Broadcast using PVCs

The following is an advanced use of AMI using a PERL script. The # sign denotes comments that offer explanations to the various lines of code. This script will create a PVC from every switch port to every other switch port, creating a broadcast.

In particular, pay close attention to the following lines of code:

- Line 8 uses AMI to retrieve network module information.
- Line 48 uses AMI to create terminating paths.
- Line 55 uses AMI to create originating paths.
- Line 60 uses AMI to create PVCs.

The following is the AMI script to create broadcast:

```
 1 #!/usr/local/bin/perl
 2 # This script works on ASX200 switches
 3 # vpi/vci to use for the interconnections
 4 $VPI = 10; $VCI = 250;
 5 # get switch name
 6 $switch = shift || die "Usage: $0 switch\n";
 7 # figure out the ports on each netmod
 8 @response = `echo "conf module show" | ami $switch`;
 9 # Netmod A
10 chop(@moduleA = grep (/^[01]A/,@response));
11 $A_mod = $moduleA[0] if $#moduleA == 0;
12 if ($A_mod =~ s/^[01](A).*/\1/) {
13    ($x, $x, $ports{$A_mod}, $x, $type{$A_mod}) = split(/\s+/,$moduleA[0]);
14    print "Netmod $A_mod is of type $type{$A_mod}\n" if $A_mod;
15    push (@netmods,"A");
16 }
#
# Repeat procedure (lines 9-16) fore netmods B, C, D
#
39 # set up a pvc from each port to all the others
40 $need_orig_path=1;
41 foreach $src_netmod (@netmods) {
42    $src_end = $ports{$src_netmod};

43   foreach $src_port (1..$src_end) {
44      # construct the first part of the ami command string
45      $ami_src_cmd = "conf vcc new $src_netmod$src_port $VPI $VCI";
46      # Create the term path
47      print "ami cmd: \"conf vpc new $src_netmod$src_port $VPI term\"\n";
48      `echo "conf vpc new $src_netmod$src_port $VPI term" | ami $switch private`;
49      foreach $dest_netmod (@netmods) {
50         $dest_end = $ports{$dest_netmod};
51         foreach $dest_port (1..$dest_end) {
52            # Create the orig path
53            if ($need_orig_path) {
54               print "ami cmd: \"conf vpc new $dest_netmod$dest_port $VPI orig\"\n";
55               `echo "conf vpc new $dest_netmod$dest_port $VPI orig" | ami $switch
private`;
56            }
57            next if ($dest_port == $src_port && $dest_netmod eq
$src_netmod);
58            $ami_dest_cmd = " $dest_netmod$dest_port $VPI $VCI";
59            print "ami cmd: \"$ami_src_cmd $ami_dest_cmd\"\n";
60            `echo "$ami_src_cmd $ami_dest_cmd" | ami $switch private`;
61          }
62       }
63       $need_orig_path=0;
64    }
65 }
```

And here is some of the output:

```
Netmod A is of type NM-B-TAXI-100-6PT
Netmod B is of type NM-C-DS3-TIMING-4PT
Netmod C is of type NM-B-E3-4PT
ami cmd: "conf vpc new A1 10 term"
ami cmd: "conf vpc new A1 10 orig"
ami cmd: "conf vpc new A2 10 orig"
ami cmd: "conf vcc new A1 10 250  A2 10 250"
ami cmd: "conf vpc new A3 10 orig"
ami cmd: "conf vcc new A1 10 250  A3 10 250"
ami cmd: "conf vpc new A4 10 orig"
ami cmd: "conf vcc new A1 10 250  A4 10 250"
ami cmd: "conf vpc new A5 10 orig"
ami cmd: "conf vcc new A1 10 250  A5 10 250"
ami cmd: "conf vpc new A6 10 orig"
ami cmd: "conf vcc new A1 10 250  A6 10 250"
ami cmd: "conf vpc new B1 10 orig"
ami cmd: "conf vcc new A1 10 250  B1 10 250"
ami cmd: "conf vpc new B2 10 orig"
ami cmd: "conf vcc new A1 10 250  B2 10 250"
ami cmd: "conf vpc new B3 10 orig"
ami cmd: "conf vcc new A1 10 250  B3 10 250"
ami cmd: "conf vpc new B4 10 orig"
ami cmd: "conf vcc new A1 10 250  B4 10 250"
ami cmd: "conf vpc new C1 10 orig"
ami cmd: "conf vcc new A1 10 250  C1 10 250"
ami cmd: "conf vpc new C2 10 orig"
ami cmd: "conf vcc new A1 10 250  C2 10 250"
ami cmd: "conf vpc new C3 10 orig"
ami cmd: "conf vcc new A1 10 250  C3 10 250"
ami cmd: "conf vpc new C4 10 orig"
ami cmd: "conf vcc new A1 10 250  C4 10 250"
ami cmd: "conf vpc new A2 10 term"
ami cmd: "conf vcc new A2 10 250  A1 10 250"
ami cmd: "conf vcc new A2 10 250  A3 10 250"
ami cmd: "conf vcc new A2 10 250  A4 10 250"
ami cmd: "conf vcc new A2 10 250  A5 10 250"
ami cmd: "conf vcc new A2 10 250  A6 10 250"
ami cmd: "conf vcc new A2 10 250  B1 10 250"
ami cmd: "conf vcc new A2 10 250  B2 10 250"
ami cmd: "conf vcc new A2 10 250  B3 10 250"
(Output truncated...)
```

APPENDIX A An Overview of Virtual Connections

ATM is a switched, connection-oriented technology in which information, in the form of cells, is transferred through the network via switched virtual connections. The components that make up virtual connections are the media, virtual paths (VPs), and virtual channels (VCs). *ForeView* provides a tool for the provisioning and management of virtual connections, the Virtual Path/Channel. This appendix discusses the concepts of virtual connections.

A.1 General Concepts

Each ATM cell contains a virtual path identifier (VPI) and a virtual channel identifier (VCI) as part of its five-byte ATM header. The VPI and VCI are used to route the cell through the ATM network. When a switch fabric receives a cell, it examines the ATM header to determine the correct output port, VPI, and VCI for the cell. For example, an ATM switch fabric can be configured such that any cell received on port A1 with VPI|VCI = 0|32 is switched to port B2 with VPI|VCI = 0|35. The translation from input port, VPI, and VCI to output port, VPI, and VCI is achieved via a mapping table in the switch fabric's memory.

The VCI value of cells does not change as the cell is switched through the ATM network via a virtual path. In a single switch environment, a cell's VPI and VCI are translated only once, but in a multiple switch environment a cell's VPI and VCI are translated many times. It is important to remember that a cell's VPI and VCI are of local significance only (i.e., link-by-link). It is also important to note that virtual connections are unidirectional; that is, they are valid in one direction only. The VPI and VCI **may** change as the cell is switched through the network.

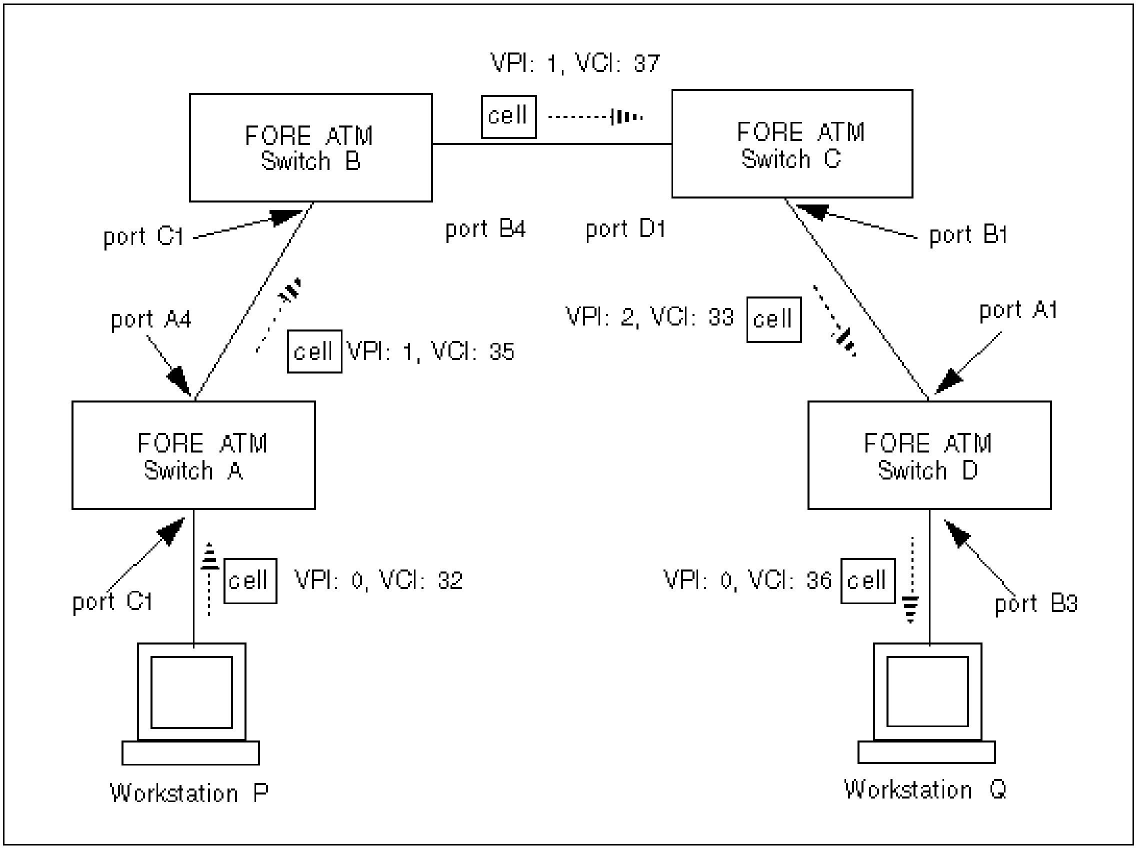


Figure A.1 - The Path of a Cell Via PVCs

The mappings in an ATM network used to route cells from a source to a destination are generally referred to as virtual channels and virtual paths. The following sections explain how to create the necessary mappings to establish these virtual paths and virtual channels in a network of FORE ATM switches.

A.2 Virtual Paths

Virtual paths, which are carried within a physical transit medium (e.g., DS1, E1, DS3, E3, OC3c, or OC12c link), are used to establish connections between two nodes in an ATM network. Many virtual paths can be transmitted within a single physical link. Two types of virtual paths exist: virtual path connections (VPCs), also known as through paths, and outgoing/incoming (originating/terminating) paths, also known as virtual path terminators (VPTs). VPCs allow virtual paths to be cross-connected at a switch node while VPTs allow virtual channels (VCCs) to be cross-connected or switched at a switch node.

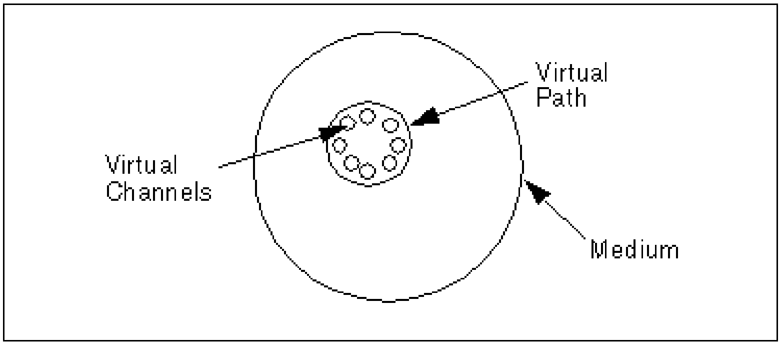


Figure A.2 - Virtual Channels in a Virtual Path

A single virtual path can be used to route many virtual channels through the ATM network. Because a virtual path simply routes virtual channels through the network, a cell is guaranteed to have the same VCI when it exits the virtual path as it had when it entered the virtual path.

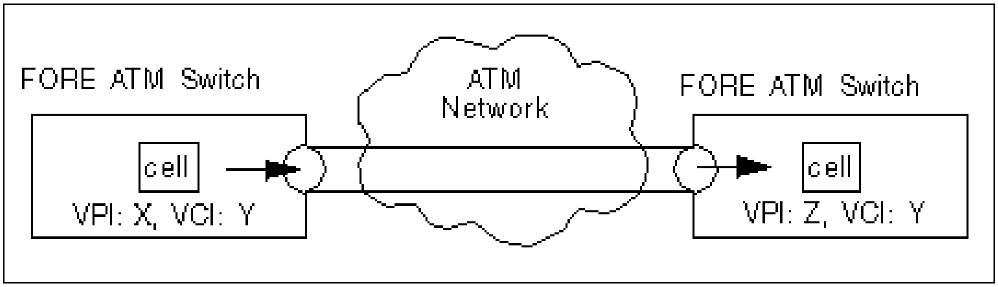


Figure A.3 - An Example of a Virtual Path

The VCI value of cells does not change as the cell is switched through the ATM network via a through path. Each virtual path must originate at a switch fabric, pass through zero or more switch fabrics and terminate at another switch fabric. The origination and termination points are referred to as outgoing and incoming paths. Virtual paths are switched through switch fabrics via through paths. Virtual paths are made up of an outgoing path, zero or more through paths, and an incoming path.

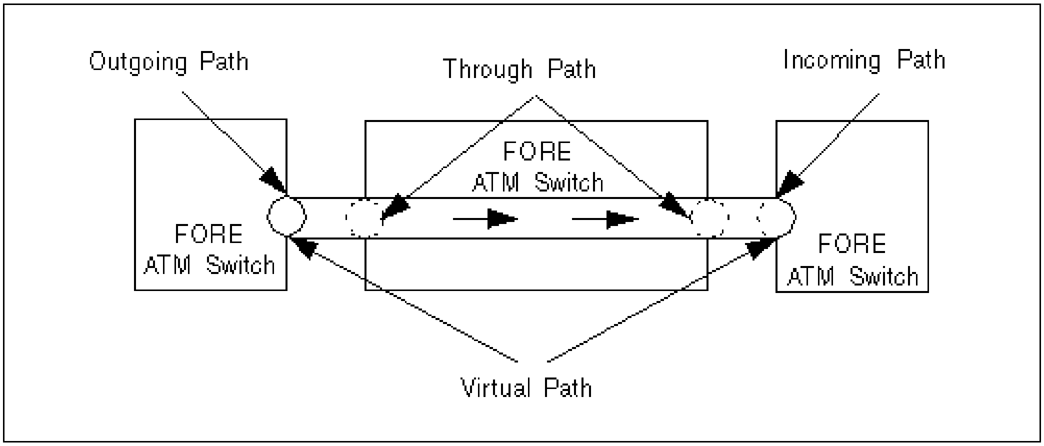


Figure A.4 - Composition of a Virtual Path

A.2.1 Through Paths (PVPs)

Through paths route an entire VPC through an ATM switch fabric. When a cell is received by a switch fabric on a through path, the VPI is examined to determine the output port and VPI. The VCI component of the ATM header remains unchanged and can have any value. So, all of the channels within the through path are switched correctly without altering the VCI value of cells on these channels.

Five parameters are needed to define a through path (PVP) on a FORE ATM switch fabric using *ForeView*: input port, input VPI, output port, and output VPI. In addition, the UPC contract is required. If left unspecified, *ForeView* defaults to UBR for the UPC contract. The VCI value remains unchanged when cells are switched via a through path. For example, the through path A4|10 -> B4|20 maps cells received on port A4 with VPI: 10 and any VCI to port B4 with VPI: 20 and the same VCI.

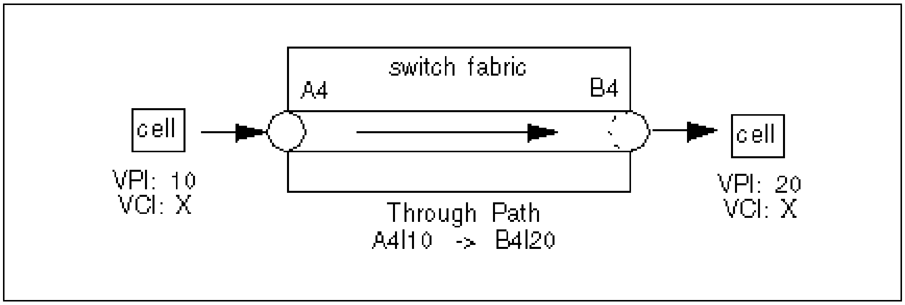


Figure A.5 - An Example of a Through Path

By definition, through paths only switch cells in one direction; they are unidirectional. For example, switch fabric X is configured with the through path B1|20 -> C1|20. If a cell is received on port C1 with VPI: 20, it is not transmitted on port B1 with a new VPI: 20. In order for this to happen, the through path C1|20 -> B1|20 must exist as well. Because through paths are unidirectional, two through paths are necessary for bidirectional communication.

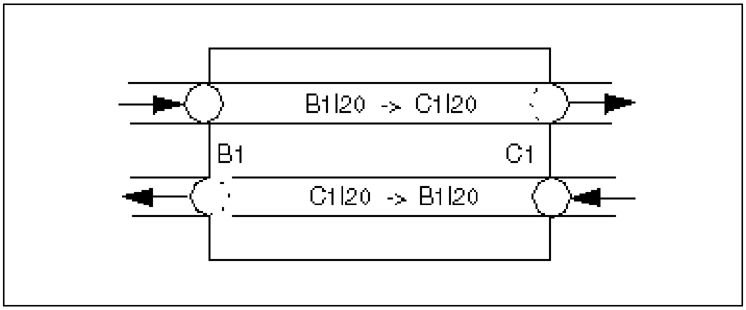


Figure A.6 - Through Paths are Unidirectional

A.2.2 Outgoing and Incoming Paths

As previously noted, outgoing (originating) and incoming (terminating) paths (also called virtual path terminators) are points at which a virtual path originates and terminates. For example, if a virtual path exists from switch fabric A to switch fabric B, then there must be an outgoing path on switch fabric A and an incoming path on switch fabric B.

An outgoing path is defined by two parameters: output VPI and output port. Similarly, an incoming path is defined by the parameters: input VPI and input port. Because outgoing and incoming paths do not define the way cells are switched through an ATM switch fabric, virtual channels must exist to switch cells from an incoming path to an outgoing path. (See the section about virtual channels for more information). Outgoing and incoming paths are the endpoints of virtual paths and are used primarily for bandwidth allocation.

The bandwidth allocated to outgoing and incoming paths is used to control the amount of virtual channel (VCC) bandwidth entering or leaving a virtual path. The total guaranteed bandwidth used by virtual channels on an outgoing path or an incoming path cannot exceed the amount of bandwidth allocated to that path. For example, as illustrated in Figure A.7, if each of the four virtual channels shown is using 10 Mbps of bandwidth, then the outgoing and incoming paths must have at least 40 Mbps of bandwidth allocated.

NOTE

UBR traffic bandwidth, which is a “best effort” service class, is not limited by the VP’s allocated bandwidth since its bandwidth is not guaranteed. Actual UBR VCC traffic transmitted within a VP may exceed the VP’s allocated bandwidth.

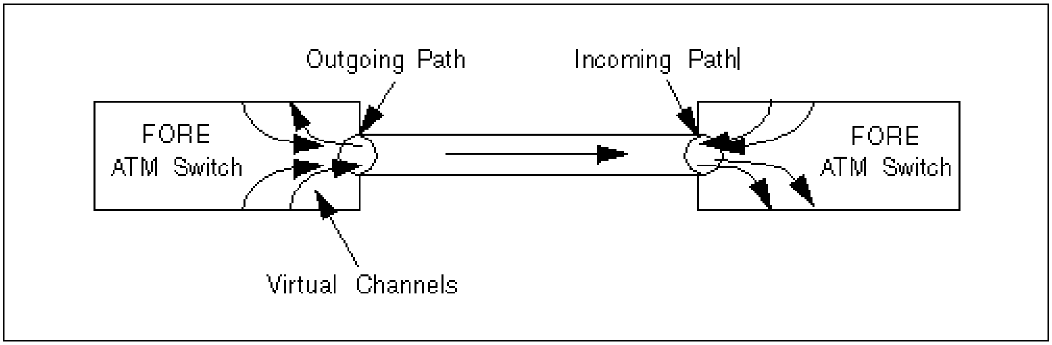


Figure A.7 - Using Outgoing and Incoming Paths for Bandwidth Allocation

A.3 Virtual Channels

Virtual channels “ride” inside of virtual paths. The combination of the two specifies a virtual connection. On a switch fabric, each virtual channel switches cells with a specific VPI and VCI received on a specific port to another port with a new VPI and a new VCI. Unlike through paths, which carry one or more VCCs, virtual channels describe a single virtual connection between two endpoints.

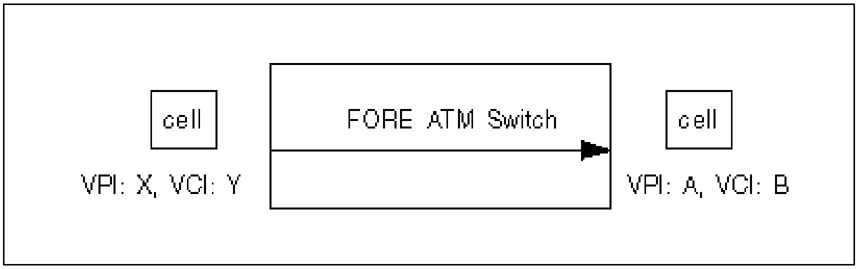


Figure A.8 - An Example of a Virtual Channel

Seven parameters are needed to define a virtual channel using *ForeView*: input port, input path, input channel, output port, output path, output channel, and the UPC contract. The UPC contract determines traffic contract, which includes the reserved bandwidth, policing action, and cell delay variation tolerance for the channel.

Virtual channels switch cells using both the VPI and VCI values. Both the VPI and VCI values may change when a cell is switched via a virtual channel. For example, the virtual channel C2|1|20 -> D2|9|25 switches cells received on port C2 with VPI: 1 and VCI: 20 such that they are transmitted out port D2 with VPI: 9 and VCI: 25.

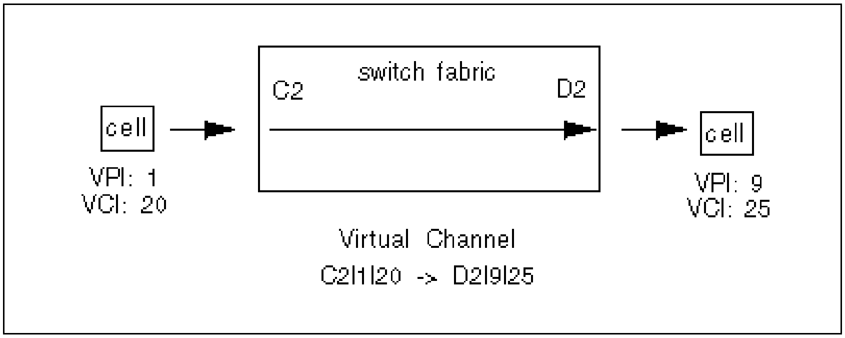


Figure A.9 - Example of a Virtual Channel

In order to establish two-way communications between two ports on a switch fabric, two virtual channels are necessary because virtual channels are unidirectional. For example, switch fabric A is configured with the virtual channel C3|7|12 -> D1|8|2. If a cell is received on port D1 with VPI: 8 and VCI: 2, it is not transmitted out port C3 with VPI: 7 and VCI: 12. An additional channel, namely D1|8|2 -> C3|7|12, would have to exist.

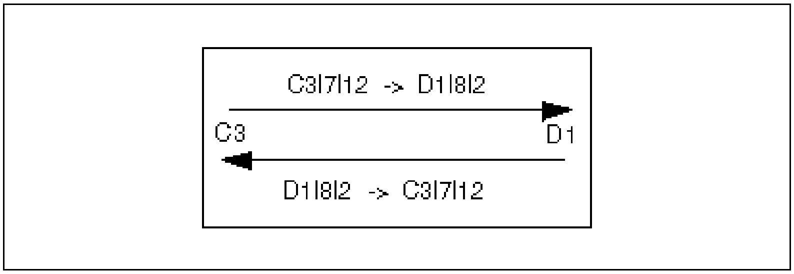


Figure A.10 - Virtual Channels are Unidirectional

Before a virtual channel can be created, the corresponding terminating and originating paths must exist. For example, before the channels shown on the switch fabric in Figure A.11 can be created, the terminating path C3|3 must exist.

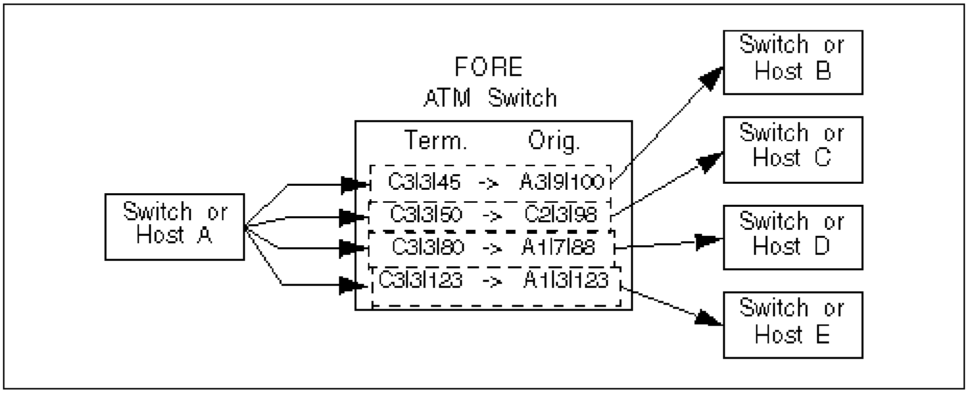


Figure A.11 - Virtual Channels Created on Terminating Path C3|3

Similarly, before the virtual channels shown in Figure A.12 can be created, the originating path C2|2 must exist.

.

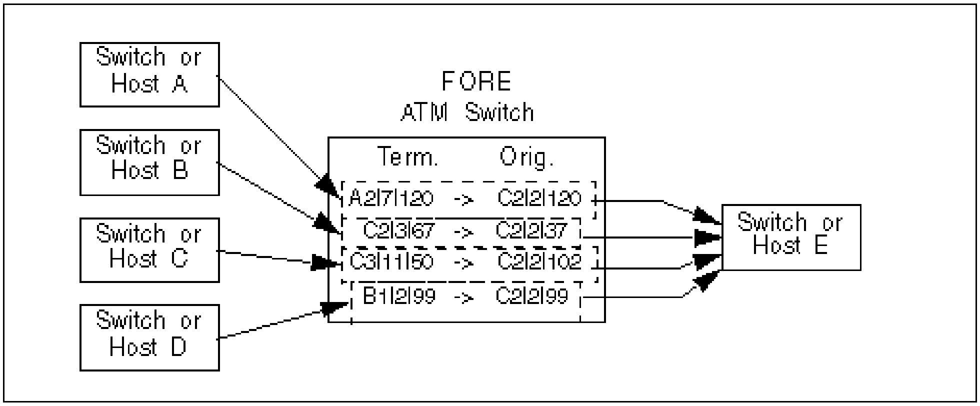


Figure A.12 - Virtual Channels Created on Originating Path C2|2

Furthermore, in these examples, the terminating path C3|3 and originating path C2|2 must have enough bandwidth allocated to support the total bandwidth used by the virtual channels.

A.4 Smart PVCs

Smart Permanent Virtual Circuits (Smart PVCs) are connections that go across multiple switch fabrics. A Smart PVC looks like a PVC at the local and remote endpoints with an SVC (Switched Virtual Circuit (or Channel)) in the middle. SVCs are channels established on demand by network signalling. Similar to a dialed telephone call, SVCs transport information between two locations and last only for the duration of the transfer.

Smart PVCs are more robust than PVCs. If a link carrying a PVC goes down, then the PVC goes down. If a link carrying a Smart PVC goes down and there is an alternate route, then the end switch fabrics of the Smart PVC automatically reroute the Smart PVC around the failed link.

In the diagram below, interswitch links exist between the *ForeRunner* switches. The endpoints exist at switch Bluefin and switch Steindachner. If a link goes down between switch Bluefin and switch Angler, a Smart PVC can reroute the cell (via an SVC) through switch Marlin.

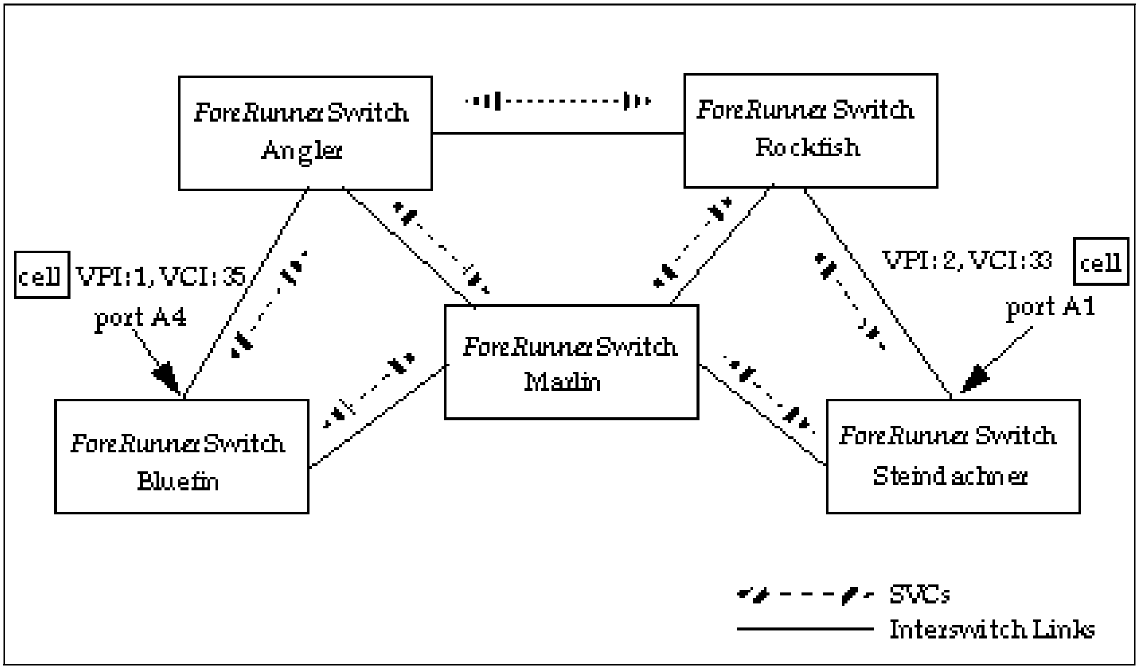


Figure A.13 - The Path of a Cell Via Smart PVCs

APPENDIX B Channel Usage in FORE ATM Networks

B.1 Signalling Channels and Reserved Paths

When configuring and browsing channels using ForeView's PVC and SPVC configuration tools, it is important to understand signalling channels used in the ATM network. When configuring new channels or deleting existing channels, **do not** reconfigure or delete any signalling channels. When monitoring or graphing channels, it is necessary to distinguish between the reserved channels used for signalling those channels set by end-users in the ATM network.

SPANS uses reserved paths/channel combinations for both UNI and NNI signalling.Current versions of SPANS reserve VPI/VCI 0/14 and 0/15 for signalling.UNI 3.x signalling uses VPI/VCI 0/5.Browsing channels on an ASX-100 or ASX-200 shows channel 0/14 and 0/15 configured on every port on which SPANS signalling protocol is running. VPI/VCI 4095/65535 is also reserved because it was used by prior versions of SPANS for signalling. SVCs created dynamically by SPANS are always on path 0 and in a channel range incrementing from 32.User-created PVCs can be on any other path and channel.

By default, *ForeView* graph, log, and trace tools that show channels show only user-created VCs. Therefore, channels 0/5, 0/14, 0/15, 4095/65535 **are not displayed**.Because they are not displayed, they cannot be inadvertently selected and used. This feature allows rapid selection of VCs that are created statically (PVCs) or dynamically (SVC) by end-users in the network.

To change from default behavior to display all channels, simply edit the .foreview configuration file (Chapter 3) ShowReserved resource. By removing the comment mark (#), the value of this resource is set to the boolean TRUE, thus adding the reserved channels to the *ForeView* utilities.

APPENDIX C SNMP Indexing

There are two main SNMP indexing schemes used to index SNMP statistics: software port indices and hardware port indices. Software port indices are single numbers starting at 0 for the first port, incrementing 4 ports per module on an ASX-100 and 8 ports per module on ASX-200 switches. For example, port A1 on an ASX-200 (A0 on an ASX-100) has a software port index of 0. Port C3 on an ASX-200 (C2 on an ASX-100) has a software port index of 18, or 8 * 2 + 2 (10 on an ASX-100, or 4 * 2 + 2).

Hardware port indices are of the form {board}.{module}.{port}. They start at 0.0.0 for the first port and increment across boards, modules, and ports. For example, port C3 on an ASX-200 (C2 on an ASX-100) is hardware port 0.2.2. Note that board numbers are zero for ASX-100s and ASX-200s. With a multi-board switch, such as the ASX-200 BXE, board numbers increment across multiple boards. Port 3A5 on an ASX-200 would be hardware index 2.0.4.

Please refer to the tables on the next two pages for a summary of the port number conventions used in *ForeRunner* switches and related SNMP indexing format.

Table C.1 - ASX-100

Port Name	Software Port Number	Board-Netmod-Port Index	Port Name	Software Port Number	Board-Netmod-Port Index
A0	0	0.0.0	C1	9	0.2.1
A1	1	0.0.1	C2	10	0.2.2
A2	2	0.0.2	C3	11	0.2.3
A3	3	0.0.3	D0	12	0.3.0
B0	4	0.1.0	D1	13	0.3.1
B1	5	0.1.1	D2	14	0.3.2
B2	6	0.1.2	D3	15	0.3.3
B3	7	0.1.3	CTL	16	0.4.0
C0	8	0.2.0			

Table C.2 - ASX-200 / ASX-200WG / ASX-200BX

Port Name	Software Port Number	Board-Netmod-Port Index	Port Name	Software Port Number	Board-Netmod-Port Index
A1	0	0.0.0	C1	16	0.2.0
A2	1	0.0.1	C2	17	0.2.1
A3	2	0.0.2	C3	18	0.2.2
A4	3	0.0.3	C4	19	0.2.3
A5	4	0.0.4	C5	20	0.2.4
A6	5	0.0.5	C6	21	0.2.5
B1	8	0.1.0	D1	24	0.3.0
B2	9	0.1.1	D2	25	0.3.1
B3	10	0.1.2	D3	26	0.3.2
B4	11	0.1.3	D4	27	0.3.3
B5	12	0.1.4	D5	28	0.3.4
B6	13	0.1.5	D6	29	0.3.5
			CTL	56	0.7.0

Table C.3 - ASX-1000

Port Name	Software Port Number	Board-Netmod-Port Index	Port Name	Software Port Number	Board-Netmod-Port Index
A1	0	0.0.0	C2	17	0.2.1
A2	1	0.0.1	C3	18	0.2.2
A3	2	0.0.2	C4	19	0.2.3
A4	3	0.0.3	C5	20	0.2.4
A5	4	0.0.4	C6	21	0.2.5
A6	5	0.0.5	C7	22	0.2.6
A7	6	0.0.6	C8	23	0.2.7
A8	7	0.0.7	D1	24	0.3.0
B1	8	0.1.0	D2	25	0.3.1
B2	9	0.1.1	D3	26	0.3.2
B3	10	0.1.2	D4	27	0.3.3
B4	11	0.1.3	D5	28	0.3.4
B5	12	0.1.4	D6	29	0.3.5
B6	13	0.1.5	D7	30	0.3.6
B7	14	0.1.6	D8	31	0.3.7
B8	15	0.1.7	CTL	56	0.7.0
C1	16	0.2.0			

APPENDIX D SNMP Traps

SNMP traps are used to update the state of the network automatically to remote network management hosts. The SNMP agent on the switch supports several SNMP traps.

The traps generated by the switch's SNMP agent can be sent to as many destinations as needed. These destinations are configurable via the ATM Management Interface (AMI). Each destination must be an IP address of a network management host. The network management host specified for a trap destination can be any host with which the switch has connectivity. This means that the host does not have to be a directly connected ATM host. It can be on any attached network. The following table describes the supported traps.

Table D.1 - SNMP Traps Supported on the ASX Switches

Trap Number	Trap Name	Description
0	asxSwLinkDown	An asxSwLinkDown trap signifies that the sending protocol entity recognizes a failure in one of the ATM Switch links that is connected to another switch.
1	asxSwLinkUp	An asxSwLinkUp trap signifies that the sending protocol entity recognizes that one of the ATM Switch links that is connected to another switch has come up.
2	asxHostLinkDown	An asxHostLinkDown trap signifies that the sending protocol entity recognizes a failure in one of ATM Switch links that is connected to a host.
3	asxHostLinkUp	An asxHostLinkUp trap signifies that the sending protocol entity recognizes that one of the ATM Switch links that is connected to a host has come up.
4	asxNetModuleDown	An asxNetModuleDown trap signifies that the sending protocol entity recognizes a failure in one of the ATM Switch network modules, that is identified by the board and the module numbers. This is probably caused by a hot-swap of a network module.

Table D.1 - SNMP Traps Supported on the ASX Switches

Trap Number	Trap Name	Description
5	asxNetModuleUp	An asxNetModuleUp trap signifies that the sending protocol entity recognizes a new operational ATM Switch network module, that is identified by the board and the module numbers. This is probably caused by a hot-swap of a network module.
6	asxPsInputDown	This trap alerts that one ATM switch power supply failed due to failure in the input voltage. The power supply that failed is identified by the power supply index. Note that an input voltage may be out of specification and may not cause a power supply failure if high loads are not applied.
7	asxPsInputUp	This trap alerts that one ATM switch power supply that had an AC input failure is up. The power supply that is back up is identified by the power supply index.
9	asxPsOutputDown	This trap alerts that one ATM switch power supply output or the power supply was physically removed. The power supply that failed is identified by the power supply index.
10	asxPsOutputUp	This trap alerts that one ATM switch power supply that had an output failure or was removed is now up. The power supply that is back up is identified by the power supply index.
22	asxFanBankDown	This trap alerts that one ATM switch fan bank failed. The fan bank that failed is identified by the fan bank index.
23	asxFanBankUp	This trap alerts that one ATM switch fan bank is up. The fan bank that is back up is identified by the fan bank index.
28	asxLinkDown	This trap alerts that the link that is identified by {hwPortBoard, hwPortModule, hwPortNumber} was configured up but lost its carrier (or the framing bit) and is currently down.

Table D.1 - SNMP Traps Supported on the ASX Switches

Trap Number	Trap Name	Description
29	asxLinkUp	This trap alerts that the link that is identified by {hwPortBoard, hwPortModule, hwPortNumber} is back up.
30	asxSpansDown	This trap alerts that the SPANS signalling on the link that is identified by the sigPathPort and sigPathVPI failed.
31	asxSpansUp	This trap alerts that the SPANS signalling on the link that is identified by the sigPathPort and sigPathVPI is up.
32	asxTempSensorOverTemp	This trap alerts that one of the temperature sensors indicates over temperature. The temperature sensor is identified by the temperature sensor index.
33	asxTempSensorRegularTemp	This trap alerts that one of the temperature sensors indicates regular temperature. The temperature sensor is identified by the temperature sensor index.
34	asxFabricTemperature-OverTemp	This trap alerts that one of the temperature sensors indicates over temperature. The temperature sensor is identified by the temperature sensor index.
35	asxFabricTemperature-RegularTemp	This trap alerts that one of the temperature sensors indicates regular temperature. The temperature sensor is identified by the temperature sensor index.
36	asxSonetLOSon	This trap indicates that the specified SONET port is experiencing Loss Of Signal. Bellcore Document TA-NWT-000253 Section 6.3.1.1.1 states that... A SONET NE shall declare a LOS failure when the LOS defect persists for 2.5 (+- .5) seconds, or when a LOS defect is present and the criteria for LOF failure declaration have been met.
37	asxSonetLOSoff	This trap indicates that the LOS condition identified by trap asxSonetLOSon has been cleared.
38	asxSonetPathLabelOn	This trap indicates that the specified SONET port is receiving and errored C2 Path Label byte. Reference Bellcore Document TA-NWT-000253 Section 3.3.2.3 and 6.3.1.1.8 the Path Label (C2) byte should have the value 0x13.

Table D.1 - SNMP Traps Supported on the ASX Switches

Trap Number	Trap Name	Description
39	asxSonetPathLabelOff	This trap indicates that the Errored Path Label (C2) byte error condition signalled by the asxSonetPathLabelOn trap has been cleared.
40	asxSonetLineAISon	This trap indicates that the specified SONET port is receiving a Line level Alarm Indication Signal from the far-end equipment.
41	asxSonetLineAISoff	This trap indicates that the Line AIS error condition signalled by the asxSonetLineAISon trap has been cleared.
42	asxDS3FERFOn	This trap indicates that the specified DS3 port is in the DS3 Yellow Alarm or FERF state. The FERF or DS3 Yellow alarm is declared if either OOF(LOF), LOS or AIS is detected and persists for 2.5+- .5 seconds.
43	asxDS3FERFOff	This trap indicates that the specified DS3 port is no longer in the FERF or DS3 Yellow Alarm state.
44	asxDS3PLCPYellowOn	This trap indicates that the specified DS3 port is in the PLCP Yellow Alarm state. The Yellow alarm is declared if PLCP LOF is detected and persists for 2.5+- .5 seconds.
45	asxDS3PLCPYellowOff	This trap indicates that the specified DS3 port is no longer in the PLCP Yellow Alarm state.
46	asxDS3PLCPYellowDetected	This trap indicates that the specified DS3 port has detected incoming Yellow Alarm.
47	asxDS3PLCPYellowCleared	This trap indicates that the specified DS3 port has detected clearance of incoming Yellow Alarm.
48	asxDS3PLCPLOFDetected	This trap indicates that the specified DS3 port has detected incoming LOF Alarm.
49	asxDS3PLCPLOFCleared	This trap indicates that the specified DS3 port has detected clearance of incoming LOF Alarm.
50	asxDS3LOFDetected	This trap indicates that Loss Of Frame(LOF) is detected on the incoming signal.
51	asxDS3LOFCleared	This trap indicates that Loss Of Frame is cleared on the incoming signal.

Table D.1 - SNMP Traps Supported on the ASX Switches

Trap Number	Trap Name	Description
52	asxDS3AISDetected	This trap indicates that AIS Alarm is detected on the incoming signal.
53	asxDS3AISCleared	This trap indicates that AIS Alarm is cleared on the incoming signal.
54	asxDS3LOSDetected	This trap indicates that LOS Alarm is detected on the incoming signal.
55	asxDS3LOSCleared	This trap indicates that LOS Alarm is cleared on the incoming signal.
56	asxDS1YellowOn	This trap indicates that the specified DS1 port is in the Yellow Alarm state. The Yellow alarm is declared if either OOF or AIS is detected and persists for 2.5+- .5 seconds.
57	asxDS1YellowOff	This trap indicates that the specified DS1 port is no longer in the Yellow Alarm state.
58	asxDS1PLCPYellowOn	This trap indicates that the specified DS1 port is in the PLCP Yellow Alarm state. The Yellow alarm is declared if PLCP LOF is detected and persists for 2.5+- .5 seconds.
59	asxDS1PLCPYellowOff	This trap indicates that the specified DS1 port is no longer in the PLCP Yellow Alarm state.
60	asxDS1PLCPYellowDetected	This trap indicates that the specified DS1 port has detected an incoming Yellow Alarm.
61	asxDS1PLCPYellowCleared	This trap indicates that the specified DS1 port has detected clearance of an incoming Yellow Alarm.
62	asxDS1PLCPLOFDetected	This trap indicates that the specified DS1 port has detected an incoming LOF Alarm.
63	asxDS1PLCPLOFCleared	This trap indicates that the specified DS1 port has detected clearance of an incoming LOF Alarm.
64	asxDS1YellowDetected	This trap indicates that Yellow Alarm is detected on the incoming signal.
65	asxDS1YellowCleared	This trap indicates that Yellow Alarm is cleared on the incoming signal.

Table D.1 - SNMP Traps Supported on the ASX Switches

Trap Number	Trap Name	Description
66	asxDS1AISDetected	This trap indicates that AIS Alarm is detected on the incoming signal.
67	asxDS1AISCleared	This trap indicates that AIS Alarm is cleared on the incoming signal.
68	asxDS1LOSDetected	This trap indicates that LOS Alarm is detected on the incoming signal.
69	asxDS1LOSCleared	This trap indicates that LOS Alarm is cleared on the incoming signal.
70	asxDS1LOFDetected	This trap indicates that LOF Alarm is detected on the incoming signal.
71	asxDS1LOFCleared	This trap indicates that LOF Alarm is cleared on the incoming signal.
74	asxDS3FERFDetected	This trap indicates that FERF Alarm is detected on the incoming signal.
75	asxDS3FERFCleared	This trap indicates that FERF Alarm is cleared on the incoming signal.
110	asxJ2YellowOn	This trap indicates that the specified J2 port is in the Yellow Alarm state. The Yellow alarm is declared if either LOF or LOS or AIS is detected and persists for 2.5+- .5 seconds.
111	asxJ2YellowOff	This trap indicates that the specified J2 port is no longer in the Yellow Alarm state.
112	asxJ2YellowDetected	This trap indicates that Yellow Alarm is detected on the incoming signal.
113	asxJ2YellowCleared	This trap indicates that Yellow Alarm is cleared on the incoming signal.
114	asxJ2AISDetected	This trap indicates that AIS Alarm is detected on the incoming signal.
115	asxJ2AISCleared	This trap indicates that AIS Alarm is cleared on the incoming signal.
116	asxJ2LOSDetected	This trap indicates that LOS Alarm is detected on the incoming signal.

Table D.1 - SNMP Traps Supported on the ASX Switches

Trap Number	Trap Name	Description
117	asxJ2LOSCleared	This trap indicates that LOS Alarm is cleared on the incoming signal.
118	asxJ2LOFDetected	This trap indicates that LOF Alarm is detected on the incoming signal.
119	asxJ2LOFCleared	This trap indicates that LOF Alarm is cleared on the incoming signal.
1024	asxOutputQueueCongested	This trap indicates that the output queue for the given priority has exceeded its dedicated length, and has begun overflowing into the shared buffer space on the network module.
1025	asxOutputQueueCellLoss	This trap indicates that the output queue for the given priority has overflowed and cells have been dropped.
1026	asxExtendedModeViolation	This trap indicates that a series A or B network module was inserted into a switch board running in extended mode.
1027	asxNonextendedMode-Warning	This trap indicates that a series C or greater network module was inserted into a switch board running in non-extended mode.
1028	q2931AVRejectTrap	This trap is generated whenever any UNI3.x with AddressValidation enabled rejects a Setup Request call more than q2931AVRejectTrapThreshold times in any given q2931AVRejectTrapPeriod.
1029	crConfMemoryOflow	This trap is generated when the allocated call record memory (as indicated by crMemoryAllocated) is exceeded.
1030	crXfrPrimaryXfrFailed	This trap is generated when the call record transfer to the primary host (as indicated by crXfrPrimaryUrl) fails.
1031	crXfrSecondaryXfrFailed	This trap is generated when the call record transfer to the secondary host (as indicated by crXfrSecondaryUrl) fails.

Table D.1 - SNMP Traps Supported on the ASX Switches

Trap Number	Trap Name	Description
1032	crConfMemAllocFail	This trap is generated when Callrecord functionality is unable to allocate memory as specified by crMemoryAllocated. This can happen when the crConfAdminStatus changes state from “off” or when the switch reboots when Callrecords is configured “on”.
1033	crGeneralFailure	This trap is generated when any of the callrecord related functionality fails for any reason. One example would be when the Callrecord Module fails to schedule an interval timer.

Acronyms

The networking terms in the following list are defined in the Glossary of this manual. Glossary items are listed alphabetically according to the full term.

AAL	ATM Adaptation Layer
ABR	Available Bit Rate
ACM	Address Complete Message
ACR	Allowable Cell Rate
ADPCM	Adaptive Differential Pulse Code Modulation
AHFG	ATM-attached Host Functional Group
AIMUX	ATM Inverse Multiplexing
AIS	Alarm Indication Signal
AMI	Alternate Mark Inversion
AMI	ATM Management Interface
ANSI	American National Standards Institute
APCM	Adaptive Pulse Code Modulation
API	Application Program Interface
APP	Application Program
APS	Automatic Protection Switching
ARP	Address Resolution Protocol
ASCII	American Standard Code for Information Interchange
ATDM	Asynchronous Time Division Multiplexing
ATM	Asynchronous Transfer Mode
AUI	Attachment User Interface
B8ZS	Bipolar 8 Zero Substitution
BCOB	Broadband Connection Oriented Bearer
BCOB-A	Bearer Class A
BCOB-C	Bearer Class C
BCOB-X	Bearer Class X
BECN	Backward Explicit Congestion Notification
BER	Bit Error Rate
BES	Bursty Errored Seconds
BGP	Border Gateway Protocol
B-ICI	B-ISDN Inter-Carrier Interface.
BIP	Bit Interleaved Parity
B-ISDN	Broadband Integrated Services Digital Network
B-ISUP	Broadband ISDN User’s Part

BITS	Building Integrated Timing Supply
BNC	Bayonet-Neill-Concelman
BPDU	Bridge Protocol Data Unit
bps	Bits per Second
BPV	Bipolar Violation
B-TE	Broadband Terminal Equipment
BUS	Broadcast and Unknown Server
CAC	Connection Admission Control
CAS	Channel Associated Signaling
CBDS	Connectionless Broadband Data Service
CBR	Constant Bit Rate
CCITT	International Telephone and Telegraph Consultative Committee
CCS	Common Channel Signaling
CDV	Cell Delay Variation
CE	Connection Endpoint
CEI	Connection Endpoint Identifier
CES	Circuit Emulation Service
CGA	Carrier Group Alarm
CIP	Carrier Identification Parameter
CIR	Committed Information Rate
CLIP	Classical IP
CLP	Cell Loss Priority
CLR	Cell Loss Ratio-1-15
CLS	Connectionless service
CMIP	Common Management Interface Protocol
CMR	Cell Misinsertion Rate
CPE	Customer Premise Equipment
CRA	Cell Rate Adaptation
CRC	Cyclic Redundancy Check
CRS	Cell Relay Service
CS	Controlled Slip, **or** Convergence Sublayer
CSU	Channel Service Unit
CTD	Cell Transfer Delay
CTS	Clear To Send
DACS	Digital Access and Cross-Connect System
DARPA	Defense Advanced Research Projects Agency
DCC	Data Country Code
DCE	Data Communications Equipment
DCS	Digital Cross-connect System
DES	Destination End Station
DFA	DXI Frame Address
DLCI	Data Link Connection Identifier

DNS	Domain Naming System
DSn	Digital Standard n (n=0, 1, 1C, 2, and 3)
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTR	Data Terminal Ready
EEPROM	Electrically Erasable Programmable Read Only Memory
EFCI	Explicit Forward Congestion Indication
EGP	Exterior Gateway Protocol
EIA	Electronics Industries Association
EISA	Extended Industry Standard Architecture
ELAN	Emulated Local Area Network
EMI	Electromagnetic Interference
EPROM	Erasable Programmable Read Only Memory
EQL	Equalization
ER	Explicit Rate
ES	End System, **or** Errored Second
ESF	Extended Super Frame
ESI	End System Identifier
EXZ	Excessive Zeroes (Error Event)
FC	Face Contact
FCC	Federal Communications Commission
FCS	Frame Check Sequence
FDDI	Fiber Distributed Data Interface
FDM	Frequency Division Multiplexing
FEBE	Far End Block Error
FEC	Forward Error Correction
FECN	Forward Explicit Congestion Notification
FERF	Far End Receive Failure
FIFO	First-In, First-Out
FRS	Frame-Relay Service
FTP	File Transfer Protocol
FT-PNNI	ForeThought PNNI
FUNI	Frame-Based UNI
GCAC	Generic Connection Admission Control
GCRA	Generic Cell Rate Algorithm
GFC	Generic Flow Control
HDB3	High Density Bipolar
HDLC	High Level Data Link Control
HEC	Header Error Control
HIPPI	High Performance Parallel Interface
HSSI	High-Speed Serial Interface
ICMP	Internet Control Message Protocol

IDU	Interface Data Unit
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
ILMI	Interim Local Management Interface
IP	Internet Protocol
IPX	Internetwork Packet Exchange
IS	Intermediate system
ISDN	Integrated Services Digital Network
ISO	International Standards Organization
ITU-T	International Telecommunication Union Telecommunication
IWF	Interworking Function
IXC	Interexchange Carriers
JPEG	Joint Photographic Experts Group
Kbps	Kilobits per second
LAN	Local Area Network
LANE	LAN Emulation
LAPB	Link Access Procedure, Balanced
LATA	Local Access and Transport Area
LBO	Line Build Out
LCV	Line Code Violations
LE_ARP	LAN Emulation Address Resolution Protocol
LEC	LAN Emulation Client
LECS	LAN Emulation Configuration Server
LES	LAN Emulation Server
LLC	Logical Link Control
LOF	Loss Of Frame
LOP	Loss Of Pointer
LOS	Loss Of Signal
LSB	Least Significant Bit
MAC	Media Access Control
MAN	Metropolitan Area Network
MAU	Media Attachment Unit
MBS	Maximum Burst Size
MCDV	Maximum Cell Delay Variance
MCLR	Maximum Cell Loss Ratio
MCR	Minimum Cell Rate
MCTD	Maximum Cell Transfer Delay
MIB	Management Information Base
MIC	Media Interface Connector
MID	Message Identifier
MMF	Multimode Fiber Optic Cable
MPEG	Motion Picture Experts Group
MPOA	Multiprotocol over ATM

MSB	Most Significant Bit
MTU	Maximum Transmission Unit
NM	Network Management Entity
NML	Network Management Layer
NMS	Network Management Station
NNI	Network-to-Network Interface or Network Node Interface
NPC	Network Parameter Control
NRZ	Non Return to Zero
NRZI	Non Return to Zero Inverted
NSAP	Network Service Access Point
NTSC	National TV Standards Committee
OAM	Operation and Maintenance Cell
OC-n	Optical Carrier level-n
OID	Object Identifier
OOF	Out-of-Frame
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First Protocol
OUI	Organizationally Unique Identifier
PAD	Packet Assembler Disassembler
PAL	Phase Alternate Line
PBX	Private Branch Exchange
PCI	Peripheral Component Interconnect
PCM	Pulse Code Modulation
PCR	Peak Cell Rate
PDN	Public Data Network
PDU	Protocol Data Unit
PHY	Physical Layer
ping	Packet Internet Groper
PLCP	Physical Layer Convergence Protocol
PLP	Packet Level Protocol
PM	Physical Medium
PMD	Physical Medium Dependent
PNNI	Private Network Node Interface or Private Network-to-Network Interface
PPP	Point-to-Point Protocol
PROM	Programmable Read-Only Memory
PRS	Primary Reference Source
PSN	Packet Switched Network
PT	Payload Type
PVC	Permanent Virtual Circuit (or Channel)
PVCC	Permanent Virtual Channel Connection
PVPC	Permanent Virtual Path Connection
QD	Queuing Delay
QoS	Quality of Service

RD	Routing Domain
RFCs	Requests For Comment
RFI	Radio Frequency Interference
RIP	Routing Information Protocol
RISC	Reduced Instruction Set Computer
RTS	Request To Send
SA	Source Address
SA	Source MAC Address
SAP	Service Access Point
SAR	Segmentation And Reassembly
SC	Structured Cabling, **or** Structured Connectors, **or** Stick and Click
SCR	Sustainable Cell Rate
SCSI	Small Computer Systems Interface
SDLC	Synchronous Data Link Control
SDU	Service Data Unit
SEAL	Simple and Efficient Adaptation Layer
SECAM	Systeme En Coleur Avec Memoire
SEL	Selector
SES	Severely Errored Seconds
SF	Super Frame
SGMP	Simple Gateway Management Protocol
SIR	Sustained Information Rate
SLIP	Serial Line IP
SMDS	Switched Multimegabit Data Service
SMF	Single Mode Fiber
SMTP	Simple Mail Transfer Protocol
SNA	Systems Network Architecture
SNAP	SubNetwork Access Protocol
SNI	Subscriber Network Interface
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SPANS	Simple Protocol for ATM Network Signalling
SPARC	Scalable Processor Architecture Reduced instruction set Computer
SPE	Synchronous Payload Envelope
SPVC	Smart PVC
SS7	Signaling System No. 7
SSCOP	Service Specific Connection Oriented Protocol
SSCS	Service Specific Convergence Sublayer
ST	Straight Tip, **or** Stick and Turn
STM	Synchronous Transfer Mode

STP	Shielded Twisted Pair, Spanning Tree Protocol
STS	Synchronous Transport Signal
SVC	Switched Virtual Circuit (or Channel)
SVCC	Switched Virtual Channel Connection
SVPC	Switched Virtual Path Connection
TAXI	Transparent Asynchronous Transmitter / Receiver Interface
TC	Transmission Convergence
TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TCR	Tagged Cell Rate
TCS	Transmission Convergence Sublayer
TDM	Time Division Multiplexing
TE	Terminal Equipment
TFTP	Trivial File Transfer Protocol
TM	Traffic Management
UAS	Unavailable Seconds
UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UNI	User-to-Network Interface
UPC	Usage Parameter Control
UTOPIA	Universal Test & Operations Interface for ATM
UTP	Unshielded Twisted Pair
VBR	Variable Bit Rate
VC	Virtual Channel (or Circuit)
VCC	Virtual Channel Connection
VCI	Virtual Channel Identifier
VCL	Virtual Channel Link
VINES	Virtual Network Software
VLAN	Virtual Local Area Network
VP	Virtual Path
VPC	Virtual Path Connection
VPDN	Virtual Private Data Network
VPI	Virtual Path Identifier
VPL	Virtual Path Link
VPN	Virtual Private Network
VPT	Virtual Path Terminator
VS/VD	Virtual Source / Virtual Destination
VT	Virtual Tributary
WAN	Wide-Area Network
ZBTSI	Zero Byte Time Slot Interchange

Glossary

10Base-T - a 10 Mbps baseband Ethernet specification utilizing twisted-pair cabling (Category 3, 4, or 5). 10BaseT, which is part of the IEEE 802.3 specification, has a distance limit of approximately 100 meters per segment.

802.1d Spanning Tree Bridging - the IEEE standard for bridging; a MAC layer standard for transparently connecting two or more LANs (often called subnetworks) that are running the same protocols and cabling. This arrangement creates an extended network, in which any two workstations on the linked LANs can share data.

802.3 Ethernet - the IEEE standard for Ethernet; a physical-layer standard that uses the CSMA / CD access method on a bus-topology LAN.

802.5 Token Ring - the IEEE physical-layer standard that uses the token-passing access method on a ring-topology LAN.

AAL Connection - an association established by the AAL between two or more next higher layer entities.

Adapter - A fitting that supplies a passage between two sets of equipment when they cannot be directly interconnected.

Adaptive Differential Pulse Code Modulation (ADPCM) - A technique that allows analog voice signals to be carried on a 32K bps digital channel. Sampling is done at 8Hz with 4 bits used to describe the difference between adjacent samples.

Adaptive Pulse Code Modulation (APCM) - A technique that effectively reduces occupied bandwidth per active speaker by reducing sampling rates during periods of overflow peak traffic.

Address - A unique identity of each network station on a LAN or WAN.

Address Complete Message (ACM) - A B-ISUP call control message from the receiving exchange to sending exchange indicating the completion of address information.

Address Mask - a bit mask used to identify which bits in an address (usually an IP address) are network significant, subnet significant, and host significant portions of the complete address. This mask is also known as the subnet mask because the subnetwork portion of the address can be determined by comparing the binary version of the mask to an IP address in that subnet. The mask holds the same number of bits as the protocol address it references.

Address Prefix - A string of 0 or more bits up to a maximum of 152 bits that is the lead portion of one or more ATM addresses.

Address Resolution - The procedure by which a client associates a LAN destination with the ATM address of another client or the BUS.

Address Resolution Protocol (ARP) - a method used to resolve higher level protocol addressing (such as IP) into the appropriate header data required for ATM; i.e., port, VPI, and VCI; also defines the AAL type to be used.

Agent - a component of network- and desktop-management software, such as SNMP, that gathers information from MIBs.

alarm - an unsolicited message from a device, typically indicating a problem with the system that requires attention.

Alarm Indication Signal (AIS) - In T1, an all ones condition used to alert a receiver that its incoming signal (or frame) has been lost. The loss of signal or frame is detected at the receiving end, and the failed signal is replaced by all the ones condition which the receiver interprets as an AIS. The normal response to this is AIS is for the receiving end to generate a yellow alarm signal as part of its transmission towards the faulty end. (The AIS itself is sometimes called a Blue Signal).

A-Law - The PCM coding and companding standard used in Europe.

Allowable Cell Rate (ACR) - parameter defined by the ATM Forum for ATM traffic management. ACR varies between the MCR and the PCR, and is dynamically controlled using congestion control mechanisms.

Alternate Mark Inversion (AMI) - A line coding format used on T1 facilities that transmits ones by alternate positive and negative pulses.

Alternate Routing - A mechanism that supports the use of a new path after an attempt to set up a connection along a previously selected path fails.

American National Standards Institute (ANSI) - a private organization that coordinates the setting and approval of some U.S. standards. It also represents the United States to the International Standards Organization.

American Standard Code for Information Interchange (ASCII) - a standard character set that (typically) assigns a 7-bit sequence to each letter, number, and selected control characters.

AppleTalk - a networking protocol developed by Apple Computer for communication between Apple's products and other computers. Independent of the network layer, AppleTalk runs on LocalTalk, EtherTalk and TokenTalk.

Application Layer - Layer seven of the ISO reference model; provides the end-user interface.

Application Program (APP) - a complete, self-contained program that performs a specific function directly for the user.

Application Program Interface (API) - a language format that defines how a program can be made to interact with another program, service, or other software; it allows users to develop custom interfaces with FORE products.

Assigned Cell - a cell that provides a service to an upper layer entity or ATM Layer Management entity (ATMM-entity).

asxmon - a FORE program that repeatedly displays the state of the switch and its active ports.

Asynchronous Time Division Multiplexing (ATDM) - a multiplexing technique in which a transmission capability is organized into a priori, unassigned time slots. The time slots are assigned to cells upon request of each application's instantaneous real need.

Asynchronous Transfer Mode (ATM) - a transfer mode in which the information is organized into cells. It is asynchronous in the sense that the recurrence of cells containing information from an individual user is not necessarily periodic.

ATM Adaptation Layer (AAL) - the AAL divides user information into segments suitable for packaging into a series of ATM cells. AAL layer types are used as follows:

AAL-1 - constant bit rate, time-dependent traffic such as voice and video
AAL-2 - still undefined; a placeholder for variable bit rate video transmission
AAL-3/4 - variable bit rate, delay-tolerant data traffic requiring some sequencing and/or error detection support (originally two AAL types, connection-oriented and connectionless, which have been combined)
AAL-5 - variable bit rate, delay-tolerant, connection-oriented data traffic requiring minimal sequencing or error detection support

ATM Address - Defined in the UNI Specification as 3 formats, each having 20 bytes in length.

ATM Forum - an international non-profit organization formed with the objective of accelerating the use of ATM products and services through a rapid convergence of interoperability specifications. In addition, the Forum promotes industry cooperation and awareness.

ATM Inverse Multiplexing (AIMUX) - A device that allows multiple T1 or E1 communications facilities to be combined into a single broadband facility for the transmission of ATM cells.

ATM Layer link - a section of an ATM Layer connection between two adjacent active ATM Layer entities (ATM-entities).

ATM Link - a virtual path link (VPL) or a virtual channel link (VCL).

ATM Management Interface (AMI) - the user interface to FORE Systems' *ForeThought* switch control software (SCS). AMI lets users monitor and change various operating configurations of FORE Systems switches and network module hardware and software, IP connectivity, and SNMP network management.

ATM Peer-to-Peer Connection - a virtual channel connection (VCC) or a virtual path connection (VPC) directly established, such as workstation-to-workstation. This setup is not commonly used in networks.

ATM Traffic Descriptor - a generic list of parameters that can be used to capture the intrinsic traffic characteristics of a requested ATM connection.

ATM User-to-User Connection - an association established by the ATM Layer to support communication between two or more ATM service users (i.e., between two or more next higher layer entities or between two or more ATM entities). The communication over an ATM Layer connection may be either bidirectional or unidirectional. The same Virtual Channel Identifier (VCI) is used for both directions of a connection at an interface.

atmarp - a FORE program that shows and manipulates ATM ARP entries maintained by the given device driver. This is also used to establish PVC connections.

ATM-attached Host Functional Group (AHFG) - The group of functions performed by an ATM-attached host that is participating in the MPOA service.

atmconfig - a FORE program used to enable or disable SPANS signaling.

atmstat - a FORE program that shows statistics gathered about a given adapter card by the device driver. These statistics include ATM layer and ATM adaptation layer cell and error counts. This can also be used to query other hosts via SNMP.

Attachment User Interface (AUI) - IEEE 802.3 interface between a media attachment unit (MAU) and a network interface card (NIC). The term AUI can also refer to the rear panel port to which an AUI cable might attach.

Auto-logout - a feature that automatically logs out a user if there has been no user interface activity for a specified length of time.

Automatic Protection Switching (APS) - Equipment installed in communications systems to detect circuit failures and automatically switch to redundant, standby equipment.

Available Bit Rate (ABR) - a type of traffic for which the ATM network attempts to meet that traffic's bandwidth requirements. It does not guarantee a specific amount of bandwidth and the end station must retransmit any information that did not reach the far end.

Backbone - the main connectivity device of a distributed system. All systems that have connectivity to the backbone connect to each other, but systems can set up private arrangements with each other to bypass the backbone to improve cost, performance, or security.

Backplane - High-speed communications line to which individual components are connected.

Backward Explicit Congestion Notification (BECN) - A Resource Management cell type generated by the network or the destination, indicating congestion or approaching congestion for traffic flowing in the direction opposite that of the BECN cell.

Bandwidth - usually identifies the capacity or amount of data that can be sent through a given circuit; may be user-specified in a PVC.

Baud - unit of signalling speed, equal to the number of discrete conditions or signal events per second. If each signal event represents only one bit, the baud rate is the same as bps; if each signal event represents more than one bit (such as a dibit), the baud rate is smaller than bps.

Bayonet-Neill-Concelman (BNC) - a bayonet-locking connector used to terminate coaxial cables. BNC is also referred to as Bayonet Network Connector.

Bipolar 8 Zero Substitution (B8ZS) - a technique used to satisfy the ones density requirements of digital T-carrier facilities in the public network while allowing 64 Kbps clear channel data. Strings of eight consecutive zeroes are replaced by an eight-bit code representing two intentional bipolar pulse code violations (000V10V1).

Bipolar Violation (BPV) - an error event on a line in which the normal pattern of alternating high (one) and low (zero) signals is disrupted. A bipolar violation is noted when two high signals occur without an intervening low signal, or vice versa.

B-ISDN Inter-Carrier Interface (B-ICI) - An ATM Forum defined specification for the interface between public ATM networks to support user services across multiple public carriers.

Bit Error Rate (BER) - A measure of transmission quality, generally shown as a negative exponent, (e.g., 10^{-7} which means 1 out of 10^{7} bits [1 out of 10,000,000 bits] are in error).

Bit Interleaved Parity (BIP) - an error-detection technique in which character bit patterns are forced into parity, so that the total number of one bits is always odd or always even. This is accomplished by the addition of a one or zero bit to each byte, as the byte is transmitted; at the other end of the transmission, the receiving device verifies the parity (odd or even) and the accuracy of the transmission.

Bit Robbing - The use of the least significant bit per channel in every sixth frame for signaling.

Bit Stuffing - A process in bit-oriented protocols where a zero is inserted into a string of ones by the sender to prevent the receiver from interpreting valid user data (the string of ones) as control characters (a Flag character for instance).

Border Gateway Protocol (BGP) - used by gateways in an internet connecting autonomous networks. It is derived from experiences learned using the EGP.

bps - bits per second

Bridge - a device that expands a Local Area Network by forwarding frames between data link layers associated with two separate cables, usually carrying a common protocol. Bridges can usually be made to filter certain packets (to forward only certain traffic).

Bridge Protocol Data Unit (BPDU) - A message type used by bridges to exchange management and control information.

Broadband - a service or system requiring transmission channels capable of supporting rates greater than the Integrated Services Digital Network (ISDN) primary rate.

Broadband Access - an ISDN access capable of supporting one or more broadband services.

Broadband Connection Oriented Bearer (BCOB) - Information in the SETUP message that indicates the type of service requested by the calling user.

BCOB-A (Bearer Class A) - Indicated by ATM end user in SETUP message for connection-oriented, constant bit rate service. The network may perform internetworking based on AAL information element (IE).

BCOB-C (Bearer Class C) - Indicated by ATM end user in SETUP message for connection-oriented, variable bit rate service. The network may perform internetworking based on AAL information element (IE).

BCOB-X (Bearer Class X) - Indicated by ATM end user in SETUP message for ATM transport service where AAL, traffic type and timing requirements are transparent to the network.

Broadband Integrated Services Digital Network (B-ISDN) - a common digital network suitable for voice, video, and high-speed data services running at rates beginning at 155 Mbps.

Broadband ISDN User's Part (B-ISUP) - A protocol used to establish, maintain and release broadband switched network connections across an SS7/ATM network.

Broadband Terminal Equipment (B-TE) - An equipment category for B-ISDN which includes terminal adapters and terminals.

Broadcast - Data transmission to all addresses or functions.

Broadcast and Unknown Server (BUS) - in an emulated LAN, the BUS is responsible for accepting broadcast, multicast, and unknown unicast packets from the LECs to the broadcast MAC address (FFFFFFFFFFFF) via dedicated point-to-point connections, and forwarding the packets to all of the members of the ELAN using a single point-to-multipoint connection.

Brouter (bridging/router) - a device that routes some protocols and bridges others based on configuration information.

Buffer - A data storage medium used to compensate of a difference in rate of data flow or time of occurrence of events when transmitting data from one device to another.

Building Integrated Timing Supply (BITS) - a master timing supply for an entire building, which is a master clock and its ancillary equipment. The BITS supplies DS1 and/or composite clock timing references for synchronization to all other clocks and timing sources in that building.

Bursty Errored Seconds (BES) - a BES contains more than 1 and fewer than 320 path coding violation error events, and no severely errored frame or AIS defects. Controlled slips are not included in determining BESs.

Bursty Second - a second during which there were at least the set number of BES threshold event errors but fewer than the set number of SES threshold event errors.

Byte - A computer-readable group of bits (normally 8 bits in length).

Call - an association between two or more users or between a user and a network entity that is established by the use of network capabilities. This association may have zero or more connections.

Carrier - a company, such as any of the "baby Bell" companies, that provide network communications services, either within a local area or between local areas.

Carrier Group Alarm (CGA) - A service alarm generated by a channel bank when an out-of-frame (OOF) condition exists for some predetermined length of time (generally 300 milliseconds to 2.5 seconds). The alarm causes the calls using a trunk to be dropped and trunk conditioning to be applied.

Carrier Identification Parameter (CIP) - A 3 or 4 digit code in the initial address message identifying the carrier to be used for the connection.

cchan - a FORE program that manages virtual channels on a *ForeRunner* switch running `asxd`.

Cell - an ATM Layer protocol data unit (PDU). The basic unit of information transported in ATM technology, each 53-byte cell contains a 5-byte header and a 48-byte payload.

Cell Delay Variation (CDV) - a quantification of cell clumping for a connection. The cell clumping CDV (yk) is defined as the difference between a cell's expected reference arrival time (ck) and its actual arrival time (ak). The expected reference arrival time (ck) of cell k of a specific connection is max. T is the reciprocal of the negotiated peak cell rate.

Cell Delineation - the protocol for recognizing the beginning and end of ATM cells within the raw serial bit stream.

Cell Header - ATM Layer protocol control information.

Cell Loss Priority (CLP) - the last bit of byte four in an ATM cell header; indicates the eligibility of the cell for discard by the network under congested conditions. If the bit is set to 1, the cell may be discarded by the network depending on traffic conditions.

Cell Loss Ratio - In a network, cell loss ratio is (1-x/y), where y is the number of cells that arrive in an interval at an ingress of the network; and x is the number of these y cells that leave at the egress of the network element.

Cell Loss Ratio (CLR) - CLR is a negotiated QoS parameter and acceptable values are network specific. The objective is to minimize CLR provided the end-system adapts the traffic to the changing ATM layer transfer characteristics. The Cell Loss Ratio is defined for a connection as: Lost Cells/Total Transmitted Cells. The CLR parameter is the value of CLR that the network agrees to offer as an objective over the lifetime of the connection. It is expressed as an order of magnitude, having a range of 10-1 to 10-15 and unspecified.

Cell Misinsertion Rate (CMR) - the ratio of cells received at an endpoint that were not originally transmitted by the source end in relation to the total number of cells properly transmitted.

Cell Rate Adaptation (CRA) - a function performed by a protocol module in which empty cells (known as unassigned cells) are added to the output stream. This is because there always must be a fixed number of cells in the output direction; when there are not enough cells to transmit, unassigned cells are added to the output data stream.

Cell Relay Service (CRS) - a carrier service which supports the receipt and transmission of ATM cells between end users in compliance with ATM standards and implementation specifications.

Cell Transfer Delay - the transit delay of an ATM cell successfully passed between two designated boundaries. See CTD.

Cell Transfer Delay (CTD) - This is defined as the elapsed time between a cell exit event at the measurement point 1 (e.g., at the source UNI) and the corresponding cell entry event at the measurement point 2 (e.g., the destination UNI) for a particular connection. The cell transfer delay between two measurement points is the sum of the total inter-ATM node transmission delay and the total ATM node processing delay.

Channel - A path or circuit along which information flows.

Channel Associated Signaling (CAS) - a form of circuit state signaling in which the circuit state is indicated by one or more bits of signaling status sent repetitively and associated with that specific circuit.

Channel Bank - A device that multiplexes many slow speed voice or data conversations onto high speed link and controls the flow.

Channel Service Unit (CSU) - An interface for digital leased lines which performs loopback testing and line conditioning.

Channelization - capability of transmitting independent signals together over a cable while still maintaining their separate identity for later separation.

Circuit - A communications link between points.

Circuit Emulation Service (CES) - The ATM Forum circuit emulation service interoperability specification specifies interoperability agreements for supporting Constant Bit Rate (CBR) traffic over ATM networks that comply with the other ATM Forum interoperability agreements. Specifically, this specification supports emulation of existing TDM circuits over ATM networks.

Classical IP (CLIP) - IP over ATM which conforms to RFC 1577.

Clear to Send (CTS) - and RS-232 modem interface control signal (sent from the modem to the DTE on pin 5) which indicates that the attached DTE may begin transmitting; issuance in response to the DTE's RTS.

Clocking - Regularly timed impulses.

Closed User Group - A subgroup of network users that can be its own entity; any member of the subgroup can only communicate with other members of that subgroup.

Coaxial Cable - Coax is a type of electrical communications medium used in the LAN environment. This cable consists of an outer conductor concentric to an inner conductor, separated from each other by insulating material, and covered by some protective outer material. This medium offers large bandwidth, supporting high data rates with high immunity to electrical interference and a low incidence of errors. Coax is subject to distance limitations and is relatively expensive and difficult to install.

Cold Start Trap - an SNMP trap which is sent after a power-cycle (see *trap*).

Collision - Overlapping transmissions that occur when two or more nodes on a LAN attempt to transmit at or about the same time.

Committed Information Rate (CIR) - CIR is the information transfer rate which a network offering Frame Relay Services (FRS) is committed to transfer under normal conditions. The rate is averaged over a minimum increment of time.

Common Channel Signaling (CCS) - A form signaling in which a group of circuits share a signaling channel. Refer to SS7.

Common Management Interface Protocol (CMIP) - An ITU-TSS standard for the message formats and procedures used to exchange management information in order to operate, administer maintain and provision a network.

Concatenation - The connection of transmission channels similar to a chain.

Concentrator - a communications device that offers the ability to concentrate many lower-speed channels into and out of one or more high-speed channels.

Configuration - The phase in which the LE Client discovers the LE Service.

Congestion Management - traffic management feature that helps ensure reasonable service for VBR connections in an ATM network, based on a priority, sustained cell rate (SCR), and peak cell rate (PCR). During times of congestion, bandwidth is reduced to the SCR, based on the priority of the connection.

Connection - the concatenation of ATM Layer links in order to provide an end-to-end information transfer capability to access points.

Connection Admission Control (CAC) - the procedure used to decide if a request for an ATM connection can be accepted based on the attributes of both the requested connection and the existing connections.

Connection Endpoint (CE) - a terminator at one end of a layer connection within a SAP.

Connection Endpoint Identifier (CEI) - an identifier of a CE that can be used to identify the connection at a SAP.

Connectionless Broadband Data Service (CBDS) - A connectionless service similar to Bellcore's SMDS defined by European Telecommunications Standards Institute (ETSI).

Connectionless Service - a type of service in which no pre-determined path or link has been established for transfer of information, supported by AAL 4.

Connectionless Service (CLS) - A service which allows the transfer of information among service subscribers without the need for end-to- end establishment procedures.

Connection-Oriented Service - a type of service in which information always traverses the same pre-established path or link between two points, supported by AAL 3.

Constant Bit Rate (CBR) - a type of traffic that requires a continuous, specific amount of bandwidth over the ATM network (e.g., digital information such as video and digitized voice).

Controlled Slip (CS) - a situation in which one frame's worth of data is either lost or replicated. A controlled slip typically occurs when the sending device and receiving device are not using the same clock.

Convergence Sublayer (CS) - a portion of the AAL. Data is passed first to the CS where it is divided into rational, fixed-length packets or PDUs (Protocol Data Units). For example, AAL 4 processes user data into blocks that are a maximum of 64 kbytes long.

Corresponding Entities - peer entities with a lower layer connection among them.

cpath - a FORE program used to manage virtual paths on a *ForeRunner* switch running asxd.

cport - a FORE program that monitors and changes the state of ports on a *ForeRunner* switch running asxd.

Cross Connection - a mapping between two channels or paths at a network device.

Customer Premise Equipment (CPE) - equipment that is on the customer side of the point of demarcation, as opposed to equipment that is on a carrier side. See also point of demarcation.

Cut Through - Establishment of a complete path for signaling and/or audio communications.

Cyclic Redundancy Check (CRC) - an error detection scheme in which a number is derived from the data that will be transmitted. By recalculating the CRC at the remote end and comparing it to the value originally transmitted, the receiving node can detect errors.

D3/D4 - Refers to compliance with AT&T TR (Technical Reference) 62411 definitions for coding, supervision, and alarm support. D3/D4 compatibility ensures support of digital PBXes, M24 services, Megacom services, and Mode 3 D3/D4 channel banks at DS-1 level.

D4 Channelization - refers to compliance with AT&T Technical Reference 62411 regarding DS1 frame layout (the sequential assignment of channels and time slot numbers within the DS1).

D4 Framed/Framing Format - in T1, a 193-bit frame format in which the 193rd bit is used for framing and signaling information (the frame/framing bit). To be considered in support of D4 Framing, a device must be able to synchronize and frame-up on the 193rd bit.

Data Communications Equipment (DCE) - a definition in the RS232C standard that describes the functions of the signals and the physical characteristics of an interface for a communication device such as a modem.

Data Country Code (DCC) - This specifies the country in which an address is registered. The codes are given in ISO 3166. The length of this field is two octets. The digits of the data country code are encoded in Binary Coded Decimal (BCD) syntax. The codes will be left justified and padded on the right with the hexadecimal value “F” to fill the two octets.

Data Link - Communications connection used to transmit data from a source to a destination.

Data Link Connection Identifier (DLCI) - connection identifier associated with frame relay packets that serves the same functions as, and translates directly to, the VPI/VCI on an ATM cell.

Data Link Layer - Layer 2 of the OSI model, responsible for encoding data and passing it to the physical medium. The IEEE divides this layer into the LLC (Logical Link Control) and MAC (Media Access Control) sublayers.

Data Set Ready (DSR) - an RS-232 modem interface control signal (sent from the modem to the DTE on pin 6) which indicates that the modem is connected to the telephone circuit. Usually a prerequisite to the DTE issuing RTS.

Data Terminal Equipment (DTE) - generally user devices, such as terminals and computers, that connect to data circuit-terminating equipment. They either generate or receive the data carried by the network.

Data Terminal Ready (DTR) - an RS232 modem interface control signal (sent from the DTE to the modem on pin 20) which indicates that the DTE is ready for data transmission and which requests that the modem be connected to the telephone circuit.

Datagram - a packet of information used in a connectionless network service that is routed to its destination using an address included in the datagram’s header.

DECnet - Digital Equipment Corporation's proprietary LAN.

Defense Advanced Research Projects Agency (DARPA) - the US government agency that funded the ARPANET.

Demultiplexing - a function performed by a layer entity that identifies and separates SDUs from a single connection to more than one connection (see *multiplexing*).

Destination End Station (DES) - An ATM termination point which is the destination for ATM messages of a connection and is used as a reference point for ABR services. See SES.

Digital Access and Cross-Connect System (DACS) - Digital switching system for routing T1 lines, and DS-0 portions of lines, among multiple T1 ports.

Digital Cross-connect System (DCS) - an electronic patch panel used to route digital signals in a central office.

Digital Standard n (0, 1, 1C, 2, and 3) (DSn) - a method defining the rate and format of digital hierarchy, with asynchronous data rates defined as follows:

DS0	64kb/s	1 voice channel
DS1	1.544Mb/s	24 DS0s
DS1C	3.152 Mb/s	2 DS1s
DS2	6.312 Mb/s	4 DS1s
DS3	44.736 Mb/s	28 DS1s

Synchronous data rates (SONET) are defined as:

STS-1/OC-1	51.84 Mb/s	28 DS1s or 1 DS3
STS-3/OC-3	155.52 Mb/s	3 STS-1s byte interleaved
STS-3c/OC-3c	155.52 Mb/s	Concatenated, indivisible payload
STS-12/OC-12	622.08 Mb/s	12 STS-1s, 4 STS-3cs, or any mixture
STS-12c/OC-12c	622.08 Mb/s	Concatenated, indivisible payload
STS-48/OC-48	2488.32 Mb/s	48 STS-1s, 16 STS-3cs, or any mixture

DIP (Dual In-line Package) Switch - a device that has two parallel rows of contacts that let the user switch electrical current through a pair of those contacts to on or off. They are used to reconfigure components and peripherals.

Domain Name Server - a computer that converts names to their corresponding Internet numbers. It allows users to telnet or FTP to the name instead of the number.

Domain Naming System (DNS) - the distributed name and address mechanism used in the Internet.

Duplex - Two way communication.

DXI - a generic phrase used in the full names of several protocols, all commonly used to allow a pair of DCE and DTE devices to share the implementation of a particular WAN protocol. The protocols define the packet formats used to transport data between DCE and DTE devices.

DXI Frame Address (DFA) - a connection identifier associated with ATM DXI packets that serves the same functions as, and translates directly to, the VPI/VCI on an ATM cell.

Dynamic Allocation - A technique in which the resources assigned for program execution are determined by criteria applied at the moment of need.

E.164 - A public network addressing standard utilizing up to a maximum of 15 digits. ATM uses E.164 addressing for public network addressing.

E1 - Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. E1 lines can be leased for private use from common carriers.

E3 - Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps. E3 lines can be leased for private use from common carriers.

Edge Device - A physical device which is capable of forwarding packets between legacy interworking interfaces (e.g., Ethernet, Token Ring, etc.) and ATM interfaces based on data-link and network layer information but which does not participate in the running of any network layer routing protocol. An Edge Device obtains forwarding descriptions using the route distribution protocol.

elarp - a FORE program that shows and manipulates MAC and ATM address mappings for LAN Emulation Clients (LECs).

elconfig - a FORE program that shows and modifies LEC configuration. Lets the user set the NSAP address of the LAN Emulation Configuration Server, display the list of Emulated LANs configured in the LECS for this host, display the list of ELANs locally configured along with the membership state of each, and locally administer ELAN membership.

Electrically Erasable Programmable Read Only Memory (EEPROM) - an EPROM that can be cleared with electrical signals rather than the traditional ultraviolet light.

Electromagnetic Interference (EMI) - signals generated and radiated by an electronic device that cause interference with radio communications, among other effects.

Electronics Industries Association (EIA) - a USA trade organization that issues its own standards and contributes to ANSI; developed RS-232. Membership includes USA manufacturers.

Embedded SNMP Agent - an SNMP agent can come in two forms: embedded or proxy. An embedded SNMP agent is integrated into the physical hardware and software of the unit.

Emulated Local Area Network (ELAN) - A logical network initiated by using the mechanisms defined by LAN Emulation. This could include ATM and legacy attached end stations.

End System (ES) - a system where an ATM connection is terminated or initiated (an originating end system initiates the connection; a terminating end system terminates the connection).

End System Identifier (ESI) - This identifier distinguishes multiple nodes at the same level in case the lower level peer group is partitioned.

End-to-End Connection - when used in reference to an ATM network, a connection that travels through an ATM network, passing through various ATM devices and with endpoints at the termination of the ATM network.

Enterprise - Terminology generally referring to customers with multiple, non-contiguous geographic locations.

Equalization (EQL) - the process of compensating for line distortions.

Erasable Programmable Read Only Memory (EPROM) - A PROM which may be erased and rewritten to perform new or different functions (normally done with a PROM burner).

Errored Second (ES) - a second during which at least one code violation occurred.

Ethernet - a 10-Mbps, coaxial standard for LANs in which all nodes connect to the cable where they contend for access.

Excessive Zeroes (EXZ) Error Event - An Excessive Zeroes error event for an AMI-coded signal is the occurrence of more than fifteen contiguous zeroes. For a B8ZS coded signal, the defect occurs when more than seven contiguous zeroes are detected.

Explicit Forward Congestion Indication (EFCI) - the second bit of the payload type field in the header of an ATM cell, the EFCI bit indicates network congestion to receiving hosts. On a congested switch, the EFCI bit is set to “1” by the transmitting network module when a certain number of cells have accumulated in the network module's shared memory buffer. When a cell is received that has its EFCI bit set to “1,” the receiving host notifies the sending host, which should then reduce its transmission rate.

Explicit Rate (ER) - The Explicit Rate is an RM-cell field used to limit the source ACR to a specific value. It is initially set by the source to a requested rate (such as PCR). It may be subsequently reduced by any network element in the path to a value that the element can sustain. ER is formatted as a rate.

Extended Industry Standard Architecture (EISA) - bus architecture for desktop computers that provides a 32-bit data passage and maintains compatibility with the ISA or AT architecture.

Extended Super Frame (ESF) - a T1 framing format that utilizes the 193rd bit as a framing bit, but whose Superframe is made up of 24 frames instead of 12 as in D4 format. ESF also provides CRC error detection and maintenance data link functions.

Exterior Gateway Protocol (EGP) - used by gateways in an internet, connecting autonomous networks.

Fairness - related to Generic Flow Control, fairness is defined as meeting all of the agreed quality of service requirements by controlling the order of service for all active connections.

Far End Block Error (FEBE) - an error detected by extracting the 4-bit FEBE field from the path status byte (G1). The legal range for the 4-bit field is between 0000 and 1000, representing zero to eight errors. Any other value is interpreted as zero errors.

Far End Receive Failure (FERF) - a line error asserted when a 110 binary pattern is detected in bits 6, 7, 8 of the K2 byte for five consecutive frames. A line FERF is removed when any pattern other than 110 is detected in these bits for five consecutive frames.

Far-End - in a relationship between two devices in a circuit, the far-end device is the one that is remote.

Face Contact (FC) - Designation for fiber optic connector designed by Nippon Telegraph and Telephone which features a movable anti-rotation key allowing good repeatable performance despite numerous mating. Normally referred to as Fiber Connector, FC actually stands for Face Contact and sometimes linked with PC (Point Contact), designated as FC or FC-PC.

FCC Part 68 - The FCC rules regulating the direct connection of non-telephone company provided equipment to the public telephone network.

Federal Communications Commission (FCC) - a board of commissioners appointed by the President under the Communications Act of 1934, with the authority to regulate all interstate telecommunications originating in the United States, including transmission over phone lines.

Fiber Distributed Data Interface (FDDI) - high-speed data network that uses fiber-optic as the physical medium. Operates in similar manner to Ethernet or Token Ring, only faster.

File Transfer Protocol (FTP) - a TCP/IP protocol that lets a user on one computer access, and transfer data to and from, another computer over a network. ftp is usually the name of the program the user invokes to accomplish this task.

First-In, First-Out (FIFO) - method of coordinating the sequential flow of data through a buffer.

Flag - a bit pattern of six binary “1”s bounded by a binary “0” at each end (forms a 0111 1110 or Hex “7E”). It is used to mark the beginning and/or end of a frame.

Flow Control - The way in which information is controlled in a network to prevent loss of data when the receiving buffer is near its capacity.

***ForeThought* PNNI (FT-PNNI) -** a FORE Systems routing and signalling protocol that uses private ATM (NSAP) addresses; a precursor to ATM Forum PNNI (see PNNI).

Forward Error Correction (FEC) - A technique used by a receiver for correcting errors incurred in transmission over a communications channel without requiring retransmission of any information by the transmitter; typically involves a convolution of the transmitted bits and the appending of extra bits by both the receiver and transmitter using a common algorithm.

Forward Explicit Congestion Notification (FECN) - Bit set by a Frame Relay network to inform data terminal equipment (DTE) receiving the frame that congestion was experienced in the path from source to destination. DTE receiving frames with the FECN bit set can request that higher-level protocols take flow control action as appropriate.

Fractional T1 - the use of bandwidth in 64Kbps increments up to 1.544Mbps from a T1 facility.

Frame - a variable length group of data bits with a specific format containing flags at the beginning and end to provide demarcation.

Frame Check Sequence (FCS) - In bit-oriented protocols, a 16-bit field that contains transmission error checking information, usually appended to the end of the frame.

Frame Relay - a fast packet switching protocol based on the LAPD protocol of ISDN that performs routing and transfer with less overhead processing than X.25.

Frame Synchronization Error - an error in which one or more time slot framing bits are in error.

Frame-Based UNI (FUNI) - An ATM switch-based interface which accepts frame-based ATM traffic and converts it into cells.

Frame-Relay Service (FRS) - A connection oriented service that is capable of carrying up to 4096 bytes per frame.

Framing - a protocol that separates incoming bits into identifiable groups so that the receiving multiplexer recognizes the grouping.

Frequency Division Multiplexing (FDM) - a method of dividing an available frequency range into parts with each having enough bandwidth to carry one channel.

Gbps - gigabits per second (billion)

Generic Cell Rate Algorithm (GCRA) - an algorithm which is employed in traffic policing and is part of the user/network service contract. The GCRA is a scheduling algorithm which ensures that cells are marked as conforming when they arrive when expected or later than expected and non-conforming when they arrive sooner than expected.

Generic Connection Admission Control (GCAC) - This is a process to determine if a link has potentially enough resources to support a connection.

Generic Flow Control (GFC) - the first four bits of the first byte in an ATM cell header. Used to control the flow of traffic across the User-to-Network Interface (UNI), and thus into the network. Exact mechanisms for flow control are still under investigation and no explicit definition for this field exists at this time. (This field is used only at the UNI; for NNI-NNI use (between network nodes), these four bits provide additional network address capacity, and are appended to the VPI field.)

GIO - a proprietary bus architecture used in certain Silicon Graphics, Inc. workstations.

Header - protocol control information located at the beginning of a protocol data unit.

Header Error Control (HEC) - a CRC code located in the last byte of an ATM cell header that is used for checking cell header integrity only.

High Density Bipolar (HDB3) - A bipolar coding method that does not allow more than 3 consecutive zeroes.

High Level Data Link Control (HDLC) - An ITU-TSS link layer protocol standard for point-to-point and multi-point communications.

High Performance Parallel Interface (HIPPI) - ANSI standard that extends the computer bus over fairly short distances at speeds of 800 and 1600 Mbps.

High-Speed Serial Interface (HSSI) - a serial communications connection that operates at speeds of up to 1.544 Mbps.

Host - In a network, the primary or controlling computer in a multiple computer installation.

HPUX - the Hewlett-Packard version of UNIX.

Hub - a device that connects several other devices, usually in a star topology.

I/O Module - FORE's interface cards for the LAX-20 LAN Access Switch, designed to connect Ethernet, Token Ring, and FDDI LANs to *ForeRunner* ATM networks.

Institute of Electrical and Electronics Engineers (IEEE) - the world's largest technical professional society. Based in the U.S., the IEEE sponsors technical conferences, symposia & local meetings worldwide, publishes nearly 25% of the world's technical papers in electrical, electronics & computer engineering, provides educational programs for members, and promotes standardization.

IEEE 802 - Standards for the interconnection of LAN computer equipment. Deals with the Data Link Layers of the ISO Reference Model for OSI.
IEEE 802.1 - Defines the high-level network interfaces such as architecture, internetworking and network management.
IEEE 802.2 - Defines the Logical Link Control interface between the Data Link and Network Layers.
IEEE 802.3 - Defines CSMA/CD (Ethernet).
IEEE 802.4 - Defines the token-passing bus.
IEEE 802.5 - Defines the Token Ring access methodology. This standard incorporates IBM's Token Ring specifications.
IEEE 802.6 - Defines Metropolitan Area Networks.
IEEE 802.7 - The broadband technical advisory group.
IEEE 802.8 - The fiber optics technical advisory group.
IEEE 802.9 - Defines integrated data and voice networks.

Integrated Services Digital Network (ISDN) - an emerging technology that is beginning to be offered by the telephone carriers of the world. ISDN combines voice and digital network services into a single medium or wire.

Interexchange Carriers (IXC) - Long-distance communications companies that provide service between Local Access Transport Areas (LATAs).

Interface Data - the unit of information transferred to/from the upper layer in a single interaction across a SAP. Each Interface Data Unit (IDU) controls interface information and may also contain the whole or part of the SDU.

Interface Data Unit (IDU) - The unit of information transferred to/from the upper layer in a single interaction across the SAP. Each IDU contains interface control information and may also contain the whole or part of the SDU.

Interim Local Management Interface (ILMI) - the standard that specifies the use of the Simple Network Management Protocol (SNMP) and an ATM management information base (MIB) to provide network status and configuration information.

Intermediate System (IS) - a system that provides forwarding functions or relaying functions or both for a specific ATM connection. OAM cells may be generated and received.

International Standards Organization (ISO) - a voluntary, non treaty organization founded in 1946 that is responsible for creating international standards in many areas, including computers and communications.

International Telephone and Telegraph Consultative Committee (CCITT) - the international standards body for telecommunications.

Internet - (note the capital "I") the largest internet in the world including large national backbone nets and many regional and local networks worldwide. The Internet uses the TCP/IP suite. Networks with only e-mail connectivity are not considered on the Internet.

internet - while an internet is a network, the term "internet" is usually used to refer to a collection of networks interconnected with routers.

Internet Addresses - the numbers used to identify hosts on an internet network. Internet host numbers are divided into two parts; the first is the network number and the second, or local, part is a host number on that particular network. There are also three classes of networks in the Internet, based on the number of hosts on a given network. Large networks are classified as Class A, having addresses in the range 1-126 and having a maximum of 16,387,064 hosts. Medium networks are classified as Class B, with addresses in the range 128-191 and with a maximum of 64,516 hosts. Small networks are classified as Class C, having addresses in the range 192-254 with a maximum of 254 hosts. Addresses are given as dotted decimal numbers in the following format:

nnn.nnn.nnn.nnn

In a Class A network, the first of the numbers is the network number, the last three numbers are the local host address.

In a Class B network, the first two numbers are the network, the last two are the local host address.

In a Class C network, the first three numbers are the network address, the last number is the local host address.

The following table summarizes the classes and sizes:

Class	First #	Max# Hosts
A	1-126	16,387,064
B	129-191	64,516
C	192-223	254

Network mask values are used to identify the network portion and the host portion of the address. Default network masks are as follows:

Class A - 255.0.0.0

Class B - 255.255.0.0

Class C - 255.255.255.0

Subnet masking is used when a portion of the host ID is used to identify a subnetwork. For example, if a portion of a Class B network address is used for a subnetwork, the mask could be set as 255.255.255.0. This would allow the third byte to be used as a subnetwork address. All hosts on the network would still use the IP address to get on the Internet.

Internet Control Message Protocol (ICMP) - the protocol that handles errors and control messages at the IP layer. ICMP is actually a part of the IP protocol layer. It can generate error messages, test packets, and informational messages related to IP.

Internet Engineering Task Force (IETF) - a large, open, international community of network designers, operators, vendors and researchers whose purpose is to coordinate the operation, management and evolution of the Internet to resolve short- and mid-range protocol and architectural issues.

Internet Protocol (IP) - a connectionless, best-effort packet switching protocol that offers a common layer over dissimilar networks.

Internetwork Packet Exchange (IPX) Protocol - a NetWare protocol similar to the Xerox Network Systems (XNS) protocol that provides datagram delivery of messages.

Interoperability - The ability of software and hardware on multiple machines, from multiple vendors, to communicate.

Interworking Function (IWF) - provides a means for two different technologies to interoperate.

IP Address - a unique 32-bit integer used to identify a device in an IP network. You will most commonly see IP addresses written in “dot” notation (e.g., 192.228.32.14).

IP Netmask - a 32-bit pattern that is combined with an IP address to determine which bits of an IP address denote the network number and which denote the host number. Netmasks are useful for sub-dividing IP networks. IP netmasks are written in “dot” notation (e.g., 255.255.0.0).

ISA Bus - a bus standard developed by IBM for expansion cards in the first IBM PC. The original bus supported a data path only 8 bits wide. IBM subsequently developed a 16-bit version for its AT class computers. The 16-bit AT ISA bus supports both 8- and 16-bit cards. The 8-bit bus is commonly called the PC/XT bus, and the 16-bit bus is called the AT bus.

Isochronous - signals carrying embedded timing information or signals that are dependent on uniform timing; usually associated with voice and/or video transmission.

International Telecommunications Union Telecommunications (ITU-T) - an international body of member countries whose task is to define recommendations and standards relating to the international telecommunications industry. The fundamental standards for ATM have been defined and published by the ITU-T (Previously CCITT).

J2 - Wide-area digital transmission scheme used predominantly in Japan that carries data at a rate of 6.312 Mbps.

Jitter - analog communication line distortion caused by variations of a signal from its reference timing position.

Joint Photographic Experts Group (JPEG) - An ISO Standards group that defines how to compress still pictures.

Jumper - a patch cable or wire used to establish a circuit, often temporarily, for testing or diagnostics; also, the devices, shorting blocks, used to connect adjacent exposed pins on a printed circuit board that control the functionality of the card.

Kbps - kilobits per second (thousand)

LAN Access Concentrator - a LAN access device that allows a shared transmission medium to accommodate more data sources than there are channels currently available within the transmission medium.

LAN Emulation Address Resolution Protocol (LE_ARP) - A message issued by a LE client to solicit the ATM address of another function.

LAN Emulation Client (LEC) - the component in an end system that performs data forwarding, address resolution, and other control functions when communicating with other components within an ELAN.

LAN Emulation Configuration Server (LECS) - the LECS is responsible for the initial configuration of LECs. It provides information about available ELANs that a LEC may join, together with the addresses of the LES and BUS associated with each ELAN.

LAN Emulation Server (LES) - the LES implements the control coordination function for an ELAN by registering and resolving MAC addresses to ATM addresses.

LAN Emulation (LANE) - technology that allows an ATM network to function as a LAN backbone. The ATM network must provide multicast and broadcast support, address mapping (MAC-to-ATM), SVC management, and a usable packet format. LANE also defines Ethernet and Token Ring ELANs.

lane - a program that provides control over the execution of the LAN Emulation Server (LES), Broadcast/Unknown Server (BUS), and LAN Emulation Configuration Server (LECS) on the local host.

Latency - The time interval between a network station seeking access to a transmission channel and that access being granted or received.

Layer Entity - an active layer within an element.

Layer Function - a part of the activity of the layer entities.

Layer Service - a capability of a layer and the layers beneath it that is provided to the upper layer entities at the boundary between that layer and the next higher layer.

Layer User Data - the information transferred between corresponding entities on behalf of the upper layer or layer management entities for which they are providing services.

le - a FORE program that implements both the LAN Emulation Server (LES) and the Broadcast/Unknown Server (BUS).

Leaky Bucket - informal cell policing term for the Generic Cell Rate Algorithm which in effect receives cells into a bucket and leaks them out at the specified or contracted rate (i.e., PCR).

Least Significant Bit (LSB) - lowest order bit in the binary representation of a numerical value.

lecs - a FORE program that implements the assignment of individual LECs to different emulated LANs.

leq - a FORE program that provides information about an ELAN. This information is obtained from the LES, and includes MAC addresses registered on the ELAN together with their corresponding ATM addresses.

Line Build Out (LBO) - Because T1 circuits require the last span to lose 15-22.5 dB, a selectable output attenuation is generally required of DTE equipment (typical selections include 0.0, 7.5 and 15 dB of loss at 772 KHz).

Line Code Violations (LCV) - Error Event. A Line Coding Violation (LCV) is the occurrence of either a Bipolar Violation (BPV) or Excessive Zeroes (EXZ) Error Event.

Link - An entity that defines a topological relationship (including available transport capacity) between two nodes in different subnetworks. Multiple links may exist between a pair of subnetworks. Synonymous with logical link.

Link Access Procedure, Balanced (LAPB) - Data link protocol in the X.25 protocol stack. LAPB is a bit-oriented protocol derived from HDLC. See also HDLC and X.25.

Link Down Trap - an SNMP trap, sent when an interface changes from a normal state to an error state, or is disconnected.

Link Layer - layer in the OSI model regarding transmission of data between network nodes.

Link Up Trap - an SNMP trap, sent when an interface changes from an error condition to a normal state.

Load Sharing - Two or more computers in a system that share the load during peak hours. During periods of non peak hours, one computer can manage the entire load with the other acting as a backup.

Local Access and Transport Area (LATA) - Geographic boundaries of the local telephone network, specified by the FCC, in which a single LEC may perform its operations. Communications outside or between LATAs are provided by IXCs.

Local Area Network (LAN) - a data network intended to serve an area of only a few square kilometers or less. Because the network is known to cover only a small area, optimizations can be made in the network signal protocols that permit higher data rates.

Logical Link Control (LLC) - protocol developed by the IEEE 802 committee for data-link-layer transmission control; the upper sublayer of the IEEE Layer 2 (OSI) protocol that complements the MAC protocol; IEEE standard 802.2; includes end-system addressing and error checking.

Loopback - a troubleshooting technique that returns a transmitted signal to its source so that the signal can be analyzed for errors. Typically, a loopback is set at various points in a line until the section of the line that is causing the problem is discovered.

looptest - program that tests an interface for basic cell reception and transmission functionality, usually used for diagnostic purposes to determine if an interface is functioning properly.

Loss Of Frame (LOF) - a type of transmission error that may occur in wide-area carrier lines.

Loss Of Pointer (LOP) - a type of transmission error that may occur in wide-area carrier lines.

Loss Of Signal (LOS) - a type of transmission error that may occur in wide-area carrier lines, or a condition declared when the DTE senses a loss of a DS1 signal from the CPE for more the 150 milliseconds (the DTE generally responds with an all ones “Blue or AIS” signal).

Management Information Base (MIB) - the set of parameters that an SNMP management station can query or set in the SNMP agent of a networked device (e.g., router).

Maximum Burst Size (MBS) - the Burst Tolerance (BT) is conveyed through the MBS which is coded as a number of cells. The BT together with the SCR and the GCRA determine the MBS that may be transmitted at the peak rate and still be in conformance with the GCRA.

Maximum Burst Tolerance - the largest burst of data that a network device is guaranteed to handle without discarding cells or packets. Bursts of data larger than the maximum burst size may be subject to discard.

Maximum Cell Delay Variance (MCDV) - This is the maximum two-point CDV objective across a link or node for the specified service category.

Maximum Cell Loss Ratio (MCLR) - This is the maximum ratio of the number of cells that do not make it across the link or node to the total number of cells arriving at the link or node.

Maximum Cell Transfer Delay (MCTD) - This is the sum of the fixed delay component across the link or node and MCDV.

Maximum Transmission Unit (MTU) - the largest unit of data that can be sent over a type of physical medium.

Mbps - megabits per second (million)

Media Access Control (MAC) - a media-specific access control protocol within IEEE 802 specifications; currently includes variations for Token Ring, token bus, and CSMA/CD; the lower sublayer of the IEEE’s link layer (OSI), which complements the Logical Link Control (LLC).

Media Attachment Unit (MAU) - device used in Ethernet and IEEE 802.3 networks that provides the interface between the AUI port of a station and the common medium of the Ethernet. The MAU, which can be built into a station or can be a separate device, performs physical layer functions including conversion of the digital data from the Ethernet interface, collision detection, and injection of bits onto the network.

Media Interface Connector (MIC) - fiber optic connector that joins fiber to the FDDI controller.

Message Identifier (MID) - message identifier used to associate ATM cells that carry segments from the same higher layer packet.

Metasignalling - an ATM Layer Management (LM) process that manages different types of signalling and possibly semipermanent virtual channels (VCs), including the assignment, removal, and checking of VCs.

Metasignalling VCs - the standardized VCs that convey metasignalling information across a User-to-Network Interface (UNI).

Metropolitan Area Network (MAN) - network designed to carry data over an area larger than a campus such as an entire city and its outlying area.

MicroChannel - a proprietary 16- or 32-bit bus developed by IBM for its PS/2 computers' internal expansion cards; also offered by others.

Minimum Cell Rate (MCR) - parameter defined by the ATM Forum for ATM traffic management, defined only for ABR transmissions and specifying the minimum value for the ACR.

Most Significant Bit (MSB) - highest order bit in the binary representation of a numerical value.

Motion Picture Experts Group (MPEG) - ISO group dealing with video and audio compression techniques and mechanisms for multiplexing and synchronizing various media streams.

MPOA Client - A device which implements the client side of one or more of the MPOA protocols, (i.e., is a SCP client and/or an RDP client. An MPOA Client is either an Edge Device Functional Group (EDFG) or a Host Behavior Functional Group (HBFG).

MPOA Server - An MPOA Server is any one of an ICFG or RSFG.

MPOA Service Area - The collection of server functions and their clients. A collection of physical devices consisting of an MPOA server plus the set of clients served by that server.

MPOA Target - A set of protocol address, path attributes, (e.g., internetwork layer QoS, other information derivable from received packet) describing the intended destination and its path attributes that MPOA devices may use as lookup keys.

Mu-Law - The PCM coding and companding standard used in Japan and North America.

Multicasting - The ability to broadcast messages to one node or a select group of nodes.

Multi-homed - a device having both an ATM and another network connection, like Ethernet.

Multimode Fiber Optic Cable (MMF) - fiber optic cable in which the signal or light propagates in multiple modes or paths. Since these paths may have varying lengths, a transmitted pulse of light may be received at different times and smeared to the point that pulses may interfere with surrounding pulses. This may cause the signal to be difficult or impossible to receive. This pulse dispersion sometimes limits the distance over which a MMF link can operate.

Multiplexing - a function within a layer that interleaves the information from multiple connections into one connection (see demultiplexing).

Multipoint Access - user access in which more than one terminal equipment (TE) is supported by a single network termination.

Multipoint-to-Multipoint Connection - a collection of associated ATM VC or VP links, and their associated endpoint nodes, with the following properties:

1. All N nodes in the connection, called Endpoints, serve as a Root Node in a Point-to-Multipoint connection to all of the (N-1) remaining endpoints.
2. Each of the endpoints can send information directly to any other endpoint, but the receiving endpoint cannot distinguish which of the endpoints is sending information without additional (e.g., higher layer) information.

Multipoint-to-Point Connection - a Point-to-Multipoint Connection may have zero bandwidth from the Root Node to the Leaf Nodes, and non-zero return bandwidth from the Leaf Nodes to the Root Node. Such a connection is also known as a Multipoint-to-Point Connection.

Multiprotocol over ATM (MPOA) - An effort taking place in the ATM Forum to standardize protocols for the purpose of running multiple network layer protocols over ATM.

Narrowband Channel - sub-voicegrade channel with a speed range of 100 to 200 bps.

National TV Standards Committee (NTSC) - Started in the US in 1953 from a specification laid down by the National Television Standards Committee. It takes the B-Y and R-Y color difference signals, attenuates them to I and Q, then modulates them using double-sideband suppressed subcarrier at 3.58MHz. The carrier reference is sent to the receiver as a burst during the back porch. An industry group that defines how television signals are encoded and transmitted in the US. (See also PAL, SECAM for non-U.S. countries).

Near-End - in a relationship between two devices in a circuit, the near-end device is the one that is local.

Network Layer - Layer three In the OSI model, the layer that is responsible for routing data across the network.

Network Management Entity (NM) - body of software in a switching system that provides the ability to manage the PNNI protocol. NM interacts with the PNNI protocol through the MIB.

Network Management Layer (NML) - an abstraction of the functions provided by systems which manage network elements on a collective basis, providing end-to-end network monitoring.

Network Management Station (NMS) - system responsible for managing a network or portion of a network by talking to network management agents, which reside in the managed nodes.

Network Module - ATM port interface cards which may be individually added to or removed from any *ForeRunner* ATM switch to provide a diverse choice of connection alternatives.

Network Parameter Control (NPC) - Defined as the set of actions taken by the network to monitor and control traffic from the NNI. Its main purpose is to protect network resources from malicious as well as unintentional misbehavior which can affect the QoS of other already established connections by detecting violations of negotiated parameters and taking appropriate actions. Refer to UPC.

Network Redundancy - Duplicated network equipment and/or data which can provide a backup in case of network failures.

Network Service Access Point (NSAP) - OSI generic standard for a network address consisting of 20 octets. ATM has specified E.164 for public network addressing and the NSAP address structure for private network addresses.

Network-to-Network Interface or Network Node Interface (NNI) - the interface between two public network pieces of equipment.

Node - A computer or other device when considered as part of a network.

Non Return to Zero (NRZ) - a binary encoding scheme in which ones and zeroes are represented by opposite and alternating high and low voltages and where there is no return to a zero (reference) voltage between encoded bits.

Non Return to Zero Inverted (NRZI) - A binary encoding scheme that inverts the signal on a “1” and leaves the signal unchanged for a “0”. (Also called transition encoding.)

Nonvolatile Storage - Memory storage that does not lose its contents when power is turned off.

NuBus - a high-speed bus used in Macintosh computers, structured so users can put a card into any slot on the board without creating conflict over the priority between those cards.

nx64K - This refers to a circuit bandwidth or speed provided by the aggregation of nx64 kbps channels (where n= integer > 1). The 64K or DS0 channel is the basic rate provided by the T Carrier systems.

Nyquist Theorem - In communications theory, a formula stating that two samples per cycle is sufficient to characterize a bandwidth limited analog signal; in other words, the sampling rate must be twice the highest frequency component of the signal (i.e., sample 4 KHz analog voice channels 8000 times per second).

Object Identifier (OID) - the address of a MIB variable.

Octet - a grouping of 8 bits; similar, but not identical to, a byte.

One’s Density - The requirement for digital transmission lines in the public switched telephone network that eight consecutive “0”s cannot be in a digital data stream; exists because repeaters and clocking devices within the network will lose timing after receiving eight “0”s in a row; a number of techniques are used to insert a “1” after every seventh-consecutive “0” (see Bit Stuffing).

Open Shortest Path First (OSPF) Protocol - a routing algorithm for IP that incorporates least-cost, equal-cost, and load balancing.

Open Systems Interconnection (OSI) - the 7-layer suite of protocols designed by ISO committees to be the international standard computer network architecture.

OpenView - Hewlett-Packard's network management software.

Operation and Maintenance (OAM) Cell - a cell that contains ATM LM information. It does not form part of the upper layer information transfer.

Optical Carrier level-n (OC-n) - The optical counterpart of STS-n (the basic rate of 51.84 Mbps on which SONET is based is referred to as OC-1 or STS-1).

Organizationally Unique Identifier (OUI) - Part of RFC 1483. A three-octet field in the SubNetwork Attachment Point (SNAP) header, identifying an organization which administers the meaning of the following two octet Protocol Identifier (PID) field in the SNAP header. Together they identify a distinct routed or bridged protocol.

Out-of-Band Management - refers to switch configuration via the serial port or over Ethernet, not ATM.

Out-of-Frame (OOF) - a signal condition and alarm in which some or all framing bits are lost.

Packet - An arbitrary collection of data grouped and transmitted with its user identification over a shared facility.

Packet Assembler Disassembler (PAD) - interface device that buffers data sent to/from character mode devices, and assembles and disassembles the packets needed for X.25 operation.

Packet Internet Groper (ping) - a program used to test reachability of destinations by sending them an ICMP echo request and waiting for a reply.

Packet Level Protocol (PLP) - Network layer protocol in the X.25 protocol stack. Sometimes called X.25 Level 3 or X.25 Protocol.

Packet Switched Network (PSN) - a network designed to carry data in the form of packets. The packet and its format is internal to that network.

Packet Switching - a communications paradigm in which packets (messages) are individually routed between hosts with no previously established communications path.

Payload Scrambling - a technique that eliminates certain bit patterns that may occur within an ATM cell payload that could be misinterpreted by certain sensitive transmission equipment as an alarm condition.

Payload Type (PT) - bits 2...4 in the fourth byte of an ATM cell header. The PT indicates the type of information carried by the cell. At this time, values 0...3 are used to identify various types of user data, values 4 and 5 indicate management information, and values 6 and 7 are reserved for future use.

Peak Cell Rate - at the PHY Layer SAP of a point-to-point VCC, the Peak Cell Rate is the inverse of the minimum inter-arrival time T0 of the request to send an ATM-SDU.

Peak Cell Rate (PCR) - parameter defined by the ATM Forum for ATM traffic management. In CBR transmissions, PCR determines how often data samples are sent. In ABR transmissions, PCR determines the maximum value of the ACR.

Peer Entities - entities within the same layer.

Peripheral Component Interconnect (PCI) - a local-bus standard created by Intel.

Permanent Virtual Channel Connection (PVCC) - A Virtual Channel Connection (VCC) is an ATM connection where switching is performed on the VPI/VCI fields of each cell. A Permanent VCC is one which is provisioned through some network management function and left up indefinitely.

Permanent Virtual Circuit (or Channel) (PVC) - a circuit or channel through an ATM network provisioned by a carrier between two endpoints; used for dedicated long-term information transport between locations.

Permanent Virtual Path Connection (PVPC) - A Virtual Path Connection (VPC) is an ATM connection where switching is performed on the VPI field only of each cell. A PVPC is one which is provisioned through some network management function and left up indefinitely.

Phase Alternate Line (PAL) - Largely a German/British development in the late 60s, used in the UK and much of Europe. The B-Y and R-Y signals are weighted to U and V, then modulated onto a double-sideband suppressed subcarrier at 4.43MHz. The V (R-Y) signal's phase is turned through 180 degrees on each alternate line. This gets rid of NTSC’s hue changes with phase errors at the expense of de-saturation. The carrier reference is sent as a burst in the back porch. The phase of the burst is alternated every line to convey the phase switching of the V signal. The burst's average phase is -V. (see NTSC for U.S.).

Physical Layer (PHY) - the actual cards, wires, and/or fiber-optic cabling used to connect computers, routers, and switches.

Physical Layer Connection - an association established by the PHY between two or more ATM-entities. A PHY connection consists of the concatenation of PHY links in order to provide an end-to-end transfer capability to PHY SAPs.

Physical Layer Convergence Protocol (PLCP) - a framing protocol that runs on top of the T1 or E1 framing protocol.

Physical Medium (PM) - Refers to the actual physical interfaces. Several interfaces are defined including STS-1, STS-3c, STS-12c, STM-1, STM-4, DS1, E1, DS2, E3, DS3, E4, FDDI-based, Fiber Channel-based, and STP. These range in speeds from 1.544Mbps through 622.08 Mbps.

Physical Medium Dependent (PMD) - a sublayer concerned with the bit transfer between two network nodes. It deals with wave shapes, timing recovery, line coding, and electro-optic conversions for fiber based links.

Plesiochronous - two signals are plesiochronous if their corresponding significant instants occur at nominally the same rate, with variations in rate constrained to specified limits.

Point of Demarcation - the dividing line between a carrier and the customer premise that is governed by strict standards that define the characteristics of the equipment on each side of the demarcation. Equipment on one side of the point of demarcation is the responsibility of the customer. Equipment on the other side of the point of demarcation is the responsibility of the carrier.

Point-to-Multipoint Connection - a collection of associated ATM VC or VP links, with associated endpoint nodes, with the following properties:

1. One ATM link, called the Root Link, serves as the root in a simple tree topology. When the Root node sends information, all of the remaining nodes on the connection, called Leaf nodes, receive copies of the information.

2. Each of the Leaf Nodes on the connection can send information directly to the Root Node. The Root Node cannot distinguish which Leaf is sending information without additional (higher layer) information. (See the following note for Phase 1.)

3. The Leaf Nodes cannot communicate directly to each other with this connection type.

Note: Phase 1 signalling does not support traffic sent from a Leaf to the Root.

Point-to-Point Connection - a connection with only two endpoints.

Point-to-Point Protocol (PPP) - Provides a method for transmitting packets over serial point-to-point links.

Policing - the function that ensures that a network device does not accept traffic that exceeds the configured bandwidth of a connection.

Port Identifier - The identifier assigned by a logical node to represent the point of attachment of a link to that node.

Presentation Layer - Sixth layer of the OSI model, providing services to the application layer.

Primary Reference Source (PRS) - Equipment that provides a timing signal whose long-term accuracy is maintained at 1 x 10 -11 or better with verification to universal coordinated time (UTC) and whose timing signal is used as the basis of reference for the control of other clocks within a network.

Primitive - an abstract, implementation-independent interaction between a layer service user and a layer service provider.

Priority - the parameter of ATM connections that determines the order in which they are reduced from the peak cell rate to the sustained cell rate in times of congestion. Connections with lower priority (4 is low, 1 is high) are reduced first.

Private Branch Exchange (PBX) - a private phone system (switch) that connects to the public telephone network and offers in-house connectivity. To reach an outside line, the user must dial a digit like 8 or 9.

Private Network Node Interface or Private Network-to-Network Interface (PNNI) - a protocol that defines the interaction of private ATM switches or groups of private ATM switches

Programmable Read-Only Memory (PROM) - a chip-based information storage area that can be recorded by an operator but erased only through a physical process.

Protocol - a set of rules and formats (semantic and syntactic) that determines the communication behavior of layer entities in the performance of the layer functions.

Protocol Control Information - the information exchanged between corresponding entities using a lower layer connection to coordinate their joint operation.

Protocol Data Unit (PDU) - a unit of data specified in a layer protocol and consisting of protocol control information and layer user data.

Proxy - the process in which one system acts for another system to answer protocol requests.

Proxy Agent - an agent that queries on behalf of the manager, used to monitor objects that are not directly manageable.

Public Data Network (PDN) - a network designed primarily for data transmission and intended for sharing by many users from many organizations.

Pulse Code Modulation (PCM) - a modulation scheme that samples the information signals and transmits a series of coded pulses to represent the data.

Q.2931 - Derived from Q.93B, the narrowband ISDN signalling protocol, an ITU standard describing the signalling protocol to be used by switched virtual circuits on ATM LANs.

Quality of Service (QoS) - Quality of Service is defined on an end-to-end basis in terms of the following attributes of the end-to-end ATM connection:

Cell Loss Ratio
Cell Transfer Delay
Cell Delay Variation

Queuing Delay (QD) - refers to the delay imposed on a cell by its having to be buffered because of unavailability of resources to pass the cell onto the next network function or element. This buffering could be a result of oversubscription of a physical link, or due to a connection of higher priority or tighter service constraints getting the resource of the physical link.

Radio Frequency Interference (RFI) - the unintentional transmission of radio signals. Computer equipment and wiring can both generate and receive RFI.

Real-Time Clock - a clock that maintains the time of day, in contrast to a clock that is used to time the electrical pulses on a circuit.

Red Alarm - In T1, a red alarm is generated for a locally detected failure such as when a condition like OOF exists for 2.5 seconds, causing a CGA, (Carrier Group Alarm).

Reduced Instruction Set Computer (RISC) - a generic name for CPUs that use a simpler instruction set than more traditional designs.

Redundancy - In a data transmission, the fragments of characters and bits that can be eliminated with no loss of information.

Registration - The address registration function is the mechanism by which Clients provide address information to the LAN Emulation Server.

Relaying - a function of a layer by means of which a layer entity receives data from a corresponding entity and transmits it to another corresponding entity.

Request To Send (RTS) - an RS-232 modem interface signal (sent from the DTE to the modem on pin 4) which indicates that the DTE has data to transmit.

Requests For Comment (RFCs) - IETF documents suggesting protocols and policies of the Internet, inviting comments as to the quality and validity of those policies. These comments are collected and analyzed by the IETF in order to finalize Internet standards.

RFC1483 - Multiprotocol Encapsulation over ATM Adaptation Layer 5.
RFC1490 - Multiprotocol Interconnect over Frame Relay.
RFC1577 - Classical IP and ARP over ATM.
RFC1755 - ATM Signaling Support for IP over ATM.

Robbed-Bit Signaling - In T1, refers to the use of the least significant bit of every word of frames 6 and 12 (D4), or 6, 12, 18, and 24 (ESF) for signaling purposes.

Route Server - A physical device that runs one or more network layer routing protocols, and which uses a route query protocol in order to provide network layer routing forwarding descriptions to clients.

Router - a device that forwards traffic between networks or subnetworks based on network layer information.

Routing Domain (RD) - A group of topologically contiguous systems which are running one instance of routing.

Routing Information Protocol (RIP) - a distance vector-based protocol that provides a measure of distance, or hops, from a transmitting workstation to a receiving workstation.

Routing Protocol - A general term indicating a protocol run between routers and/or route servers in order to exchange information used to allow computation of routes. The result of the routing computation will be one or more forwarding descriptions.

SBus - hardware interface for add-in boards in later-version Sun 3 workstations.

Scalable Processor Architecture Reduced instruction set Computer (SPARC) - a powerful workstation similar to a reduced-instruction-set-computing (RISC) workstation.

Segment - a single ATM link or group of interconnected ATM links of an ATM connection.

Segmentation And Reassembly (SAR) - the SAR accepts PDUs from the CS and divides them into very small segments (44 bytes long). If the CS-PDU is less than 44 bytes, it is padded to 44 with zeroes. A two-byte header and trailer are added to this basic segment. The header identifies the message type (beginning, end, continuation, or single) and contains sequence numbering and message identification. The trailer gives the SAR-PDU payload length, exclusive of pad, and contains a CRC check to ensure the SAR-PDU integrity. The result is a 48-byte PDU that fits into the payload field of an ATM cell.

Selector (SEL) - A subfield carried in SETUP message part of ATM endpoint address Domain specific Part (DSP) defined by ISO 10589, not used for ATM network routing, used by ATM end systems only.

Semipermanent Connection - a connection established via a service order or via network management.

Serial Line IP (SLIP) - A protocol used to run IP over serial lines, such as telephone circuits or RS-232 cables, interconnecting two systems.

Service Access Point (SAP) - the point at which an entity of a layer provides services to its LM entity or to an entity of the next higher layer.

Service Data Unit (SDU) - a unit of interface information whose identity is preserved from one end of a layer connection to the other.

Service Specific Connection Oriented Protocol (SSCOP) - an adaptation layer protocol defined in ITU-T Specification: Q.2110.

Service Specific Convergence Sublayer (SSCS) - The portion of the convergence sublayer that is dependent upon the type of traffic that is being converted.

Session Layer - Layer 5 in the OSI model that is responsible for establishing and managing sessions between the application programs running in different nodes.

Severely Errored Seconds (SES) - a second during which more event errors have occurred than the SES threshold (normally 10-3).

Shaping Descriptor - *n* ordered pairs of GCRA parameters (I,L) used to define the negotiated traffic shape of an APP connection. The traffic shape refers to the load-balancing of a network, where load-balancing means configuring data flows to maximize network efficiency.

Shielded Pair - Two insulated wires in a cable wrapped with metallic braid or foil to prevent interference and provide noise free transmission.

Shielded Twisted Pair (STP) - two or more insulated wires, twisted together and then wrapped in a cable with metallic braid or foil to prevent interference and offer noise-free transmissions.

Signaling System No. 7 (SS7) - The SS7 protocol has been specified by ITU-T and is a protocol for interexchange signaling.

Simple and Efficient Adaptation Layer (SEAL) - also called AAL 5, this ATM adaptation layer assumes that higher layer processes will provide error recovery, thereby simplifying the SAR portion of the adaptation layer. Using this AAL type packs all 48 bytes of an ATM cell information field with data. It also assumes that only one message is crossing the UNI at a time. That is, multiple end-users at one location cannot interleave messages on the same VC, but must queue them for sequential transmission.

Simple Gateway Management Protocol (SGMP) - the predecessor to SNMP.

Simple Mail Transfer Protocol (SMTP) - the Internet electronic mail protocol used to transfer electronic mail between hosts.

Simple Network Management Protocol (SNMP) - the Internet standard protocol for managing nodes on an IP network.

Simple Protocol for ATM Network Signalling (SPANS) - FORE Systems' proprietary signalling protocol used for establishing SVCs between FORE Systems equipment.

Single Mode Fiber (SMF) - Fiber optic cable in which the signal or light propagates in a single mode or path. Since all light follows the same path or travels the same distance, a transmitted pulse is not dispersed and does not interfere with adjacent pulses. SMF fibers can support longer distances and are limited mainly by the amount of attenuation. Refer to MMF.

Small Computer Systems Interface (SCSI) - a standard for a controller bus that connects hardware devices to their controllers on a computer bus, typically used in small systems.

Smart PVC (SPVC) - a generic term for any communications medium which is permanently provisioned at the end points, but switched in the middle. In ATM, there are two kinds of SPVCs: smart permanent virtual path connections (SPVPCs) and smart permanent virtual channel connections (SPVCCs).

snmpd - an SMNP agent for a given adapter card.

Source - Part of communications system which transmits information.

Source Address (SA) - The address from which the message or data originated.

Source MAC Address (SA) - A six octet value uniquely identifying an end point and which is sent in an IEEE LAN frame header to indicate source of frame.

Source Traffic Descriptor - a set of traffic parameters belonging to the ATM Traffic Descriptor used during the connection set-up to capture the intrinsic traffic characteristics of the connection requested by the source.

Spanning Tree Protocol - provides loop-free topology in a network environment where there are redundant paths.

Static Route - a route that is entered manually into the routing table.

Statistical Multiplexing - a technique for allowing multiple channels and paths to share the same link, typified by the ability to give the bandwidth of a temporarily idle channel to another channel.

Stick and Click (SC) - Designation for an Optical Connector featuring a 2.5 mm physically contacting ferrule with a push-pull mating design. Commonly referred to as Structured Cabling, Structured Connectors or Stick and Click

Stick and Turn (ST) - A fiber-optic connector designed by AT&T which uses the bayonet style coupling rather than screw-on as the SMA uses. The ST is generally considered the eventual replacement for the SMA type connector.

Store-and-Forward - the technique of receiving a message, storing it until the proper outgoing line is available, then retransmitting it, with no direct connection between incoming and outgoing lines.

Straight Tip (ST) - see *Stick and Turn*.

Structured Cabling (SC) - see *Stick and Click.*

Structured Connectors (SC) - see *Stick and Click*.

Sublayer - a logical subdivision of a layer.

SubNetwork Access Protocol (SNAP) - a specially reserved variant of IEEE 802.2 encoding SNAP indicates to look further into the packet where it will fine a Type field.

Subscriber Network Interface (SNI) - the interface between an SMDS end user's CPE and the network directly serving the end user, supported by either a DS1 or DS3 access arrangement.

Super Frame (SF) - a term used to describe the repeating 12 D4 frame format that composes a standard (non-ESF) T1 service.

Super User - a login ID that allows unlimited access to the full range of a device's functionality, including especially the ability to reconfigure the device and set passwords.

Sustainable Cell Rate (SCR) - ATM Forum parameter defined for traffic management. For VBR connections, SCR determines the long-term average cell rate that can be transmitted.

Sustained Information Rate (SIR) - In ATM this refers to the long-term average data transmission rate across the User-to-Network Interface. In SMDS this refers to the committed information rate (similar to CIR for Frame Relay Service).

Switch - Equipment used to interconnect lines and trunks.

Switched Connection - A connection established via signaling.

Switched Multimegabit Data Service (SMDS) - a high-speed, datagram-based, public data network service expected to be widely used by telephone companies in their data networks.

Switched Virtual Channel Connection (SVCC) - A Switched VCC is one which is established and taken down dynamically through control signaling. A Virtual Channel Connection (VCC) is an ATM connection where switching is performed on the VPI/VCI fields of each cell.

Switched Virtual Circuit (or Channel) (SVC) - a channel established on demand by network signalling, used for information transport between two locations and lasting only for the duration of the transfer; the datacom equivalent of a dialed telephone call.

Switched Virtual Path Connection (SVPC) - a connection which is established and taken down dynamically through control signaling. A Virtual Path Connection (VPC) is an ATM connection where switching is performed on the VPI field only of each cell.

Switching System - A set of one or more systems that act together and appear as a single switch for the purposes of PNNI routing.

Symmetric Connection - a connection with the same bandwidth specified for both directions.

Synchronous - signals that are sourced from the same timing reference and hence are identical in frequency.

Synchronous Data Link Control (SDLC) - IBM's data link protocol used in SNA networks.

Synchronous Optical Network (SONET) - a body of standards that defines all aspects of transporting and managing digital traffic over optical facilities in the public network.

Synchronous Payload Envelope (SPE) - the payload field plus a little overhead of a basic SONET signal.

Synchronous Transfer Mode (STM) - a transport and switching method that depends on information occurring in regular, fixed patterns with respect to a reference such as a frame pattern.

Synchronous Transport Signal (STS) - a SONET electrical signal rate.

Systeme En Coleur Avec Memoire (SECAM) - Sequential and Memory Color Television - Started in France in the late 60s, and used by other countries with a political affiliation. This is. The B-Y and R-Y signals are transmitted on alternate lines modulated on an FM subcarrier. The memory is a one line delay line in the receiver to make both color difference signals available at the same time on all lines. Due to FM, the signal is robust in difficult terrain.

Systems Network Architecture (SNA) - a proprietary networking architecture used by IBM and IBM-compatible mainframe computers.

T1 - a specification for a transmission line. The specification details the input and output characteristics and the bandwidth. T1 lines run at 1.544 Mbps and provide for 24 data channels. In common usage, the term “T1” is used interchangeably with “DS1.”

T1 Link - A wideband digital carrier facility used for transmission of digitized voice, digital data, and digitized image traffic. This link is composed of two twisted-wire pairs that can carry 24 digital channels, each operating at 64K bps at the aggregate rate of 1.544M bps, full duplex. Also referred to as DS-1.

T3 - a specification for a transmission line, the equivalent of 28 T1 lines. T3 lines run at 44.736 Mbps. In common usage, the term “T3” is used interchangeably with “DS3.”

Tachometer - in *ForeView*, the tachometer shows the level of activity on a given port. The number in the tachometer shows the value of a chosen parameter in percentage, with a colored bar providing a semi-logarithmic representation of that percentage.

Tagged Cell Rate (TCR) - An ABR service parameter, TCR limits the rate at which a source may send out-of-rate forward RM-cells. TCR is a constant fixed at 10 cells/second.

Telephony - The conversion of voices and other sounds into electrical signals which are then transmitted by telecommunications media.

Telnet - a TCP/IP protocol that defines a client/server mechanism for emulating directly-connected terminal connections.

Terminal Equipment (TE) - Terminal equipment represents the endpoint of ATM connection(s) and termination of the various protocols within the connection(s).

Throughput - Measurement of the total useful information processed or communicated by a computer during a specified time period, i.e. packets per second.

Time Division Multiplexing (TDM) - a method of traditional digital multiplexing in which a signal occupies a fixed, repetitive time slot within a higher-rate signal.

Token Ring - a network access method in which the stations circulate a token. Stations with data to send must have the token to transmit their data.

topology - a program that displays the topology of a FORE Systems ATM network. An updated topology can be periodically re-displayed by use of the interval command option.

Traffic - the calls being sent and received over a communications network. Also, the packets that are sent on a data network.

Traffic Management (TM) - The traffic control and congestion control procedures for ATM. ATM layer traffic control refers to the set of actions taken by the network to avoid congestion conditions. ATM layer congestion control refers to the set of actions taken by the network to minimize the intensity, spread and duration of congestion. The following functions form a framework for managing and controlling traffic and congestion in ATM networks and may be used in appropriate combinations:

Connection Admission Control
Feedback Control
Usage Parameter Control
Priority Control
Traffic Shaping
Network Resource Management
Frame Discard
ABR Flow Control

Traffic Parameter - A parameter for specifying a particular traffic aspect of a connection.

Trailer - the protocol control information located at the end of a PDU.

Transit Delay - the time difference between the instant at which the first bit of a PDU crosses one designated boundary, and the instant at which the last bit of the same PDU crosses a second designated boundary.

Transmission Control Protocol (TCP) - a specification for software that bundles and unbundles sent and received data into packets, manages the transmission of packets on a network, and checks for errors.

Transmission Control Protocol/Internet Protocol (TCP/IP) - a set of communications protocols that has evolved since the late 1970s, when it was first developed by the Department of Defense. Because programs supporting these protocols are available on so many different computer systems, they have become an excellent way to connect different types of computers over networks.

Transmission Convergence (TC) - generates and receives transmission frames and is responsible for all overhead associated with the transmission frame. The TC sublayer packages cells into the transmission frame.

Transmission Convergence Sublayer (TCS) - This is part of the ATM physical layer that defines how cells will be transmitted by the actual physical layer.

Transparent Asynchronous Transmitter/Receiver Interface (TAXI) - Encoding scheme used for FDDI LANs as well as for ATM; supports speed typical of 100 Mbps over multimode fiber.

Transport Layer - Layer Four of the OSI reference model that is responsible for maintaining reliable end-to-end communications across the network.

trap - a program interrupt mechanism that automatically updates the state of the network to remote network management hosts. The SNMP agent on the switch supports these SNMP traps.

Trivial File Transfer Protocol (TFTP) - Part of IP, a simplified version of FTP that allows files to be transferred from one computer to another over a network.

Twisted Pair - Insulated wire in which pairs are twisted together. Commonly used for telephone connections, and LANs because it is inexpensive.

Unassigned Cells - a generated cell identified by a standardized virtual path identifier (VPI) and virtual channel identifier (VCI) value, which does not carry information from an application using the ATM Layer service.

Unavailable Seconds (UAS) - a measurement of signal quality. Unavailable seconds start accruing when ten consecutive severely errored seconds occur.

UNI 3.0/3.1 - the User-to-Network Interface standard set forth by the ATM Forum that defines how private customer premise equipment interacts with private ATM switches.

Unicasting - The transmit operation of a single PDU by a source interface where the PDU reaches a single destination.

Universal Test & Operations Interface for ATM (UTOPIA) - Refers to an electrical interface between the TC and PMD sublayers of the PHY layer.

Unshielded Twisted Pair (UTP) - a cable that consists of two or more insulated conductors in which each pair of conductors are twisted around each other. There is no external protection and noise resistance comes solely from the twists.

Unspecified Bit Rate (UBR) - a type of traffic that is not considered time-critical (e.g., ARP messages, pure data), allocated whatever bandwidth is available at any given time. UBR traffic is given a “best effort” priority in an ATM network with no guarantee of successful transmission.

Uplink - Represents the connectivity from a border node to an upnode.

Usage Parameter Control (UPC) - mechanism that ensures that traffic on a given connection does not exceed the contracted bandwidth of the connection, responsible for policing or enforcement. UPC is sometimes confused with congestion management (see *congestion management*).

User Datagram Protocol (UDP) - the TCP/IP transaction protocol used for applications such as remote network management and name-service access; this lets users assign a name, such as “RVAX*2,S,” to a physical or numbered address.

User-to-Network Interface (UNI) - the physical and electrical demarcation point between the user and the public network service provider.

V.35 - ITU-T standard describing a synchronous, physical layer protocol used for communications between a network access device and a packet network. V.35 is most commonly used in the United States and Europe, and is recommended for speeds up to 48 Kbps.

Variable Bit Rate (VBR) - a type of traffic that, when sent over a network, is tolerant of delays and changes in the amount of bandwidth it is allocated (e.g., data applications).

Virtual Channel (or Circuit) (VC) - a communications path between two nodes identified by label rather than fixed physical path.

Virtual Channel Connection (VCC) - a unidirectional concatenation of VCLs that extends between the points where the ATM service users access the ATM Layer. The points at which the ATM cell payload is passed to, or received from, the users of the ATM Layer (i.e., a higher layer or ATMM-entity) for processing signify the endpoints of a VCC.

Virtual Channel Identifier (VCI) - the address or label of a VC; a value stored in a field in the ATM cell header that identifies an individual virtual channel to which the cell belongs. VCI values may be different for each data link hop of an ATM virtual connection.

Virtual Channel Link (VCL) - a means of unidirectional transport of ATM cells between the point where a VCI value is assigned and the point where that value is translated or removed.

Virtual Channel Switch - a network element that connects VCLs. It terminates VPCs and translates VCI values. The Virtual Channel Switch is directed by Control Plane functions and relays the cells of a VC.

Virtual Connection - an endpoint-to-endpoint connection in an ATM network. A virtual connection can be either a virtual path or a virtual channel.

Virtual Local Area Network (VLAN) - Work stations connected to an intelligent device which provides the capabilities to define LAN membership.

Virtual Network Software (VINES) - Banyan's network operating system based on UNIX and its protocols.

Virtual Path (VP) - a unidirectional logical association or bundle of VCs.

Virtual Path Connection (VPC) - a concatenation of VPLs between virtual path terminators (VPTs). VPCs are unidirectional.

Virtual Path Identifier (VPI) - the address or label of a particular VP; a value stored in a field in the ATM cell header that identifies an individual virtual path to which the cell belongs. A virtual path may comprise multiple virtual channels.

Virtual Path Link (VPL) - a means of unidirectional transport of ATM cells between the point where a VPI value is assigned and the point where that value is translated or removed.

Virtual Path Switch - a network element that connects VPLs, it translates VPI (not VCI) values and is directed by Control Plane functions. The Virtual Path Switch relays the cells of a Virtual Path.

Virtual Path Terminator (VPT) - a system that unbundles the VCs of a VP for independent processing of each VC.

Virtual Private Data Network (VPDN) - a private data communications network built on public switching and transport facilities rather than dedicated leased facilities such as T1s.

Virtual Private Network (VPN) - a private voice communications network built on public switching and transport facilities rather than dedicated leased facilities such as T1s.

Virtual Source/Virtual Destination (VS/VD) - An ABR connection may be divided into two or more separately controlled ABR segments. Each ABR control segment, except the first, is sourced by a virtual source. A virtual source implements the behavior of an ABR source endpoint. Backwards RM-cells received by a virtual source are removed from the connection. Each ABR control segment, except the last, is terminated by a virtual destination. A virtual destination assumes the behavior of an ABR destination endpoint. Forward RM-cells received by a virtual destination are turned around and not forwarded to the next segment of the connection.

Virtual Tributary (VT) - a structure used to carry payloads such as DS1s that run at significantly lower rates than STS-1s.

Warm Start Trap - an SNMP trap which indicates that SNMP alarm messages or agents have been enabled.

Wide-Area Network (WAN) - a network that covers a large geographic area.

Wideband Channel - Communications channel with more capacity (19.2K bps) than the standard capacity of a voice grade line.

X.21 - ITU-T standard for serial communications over synchronous digital lines. The X.21 protocol is used primarily in Europe and Japan.

X.25 - a well-established data switching and transport method that relies on a significant amount of processing to ensure reliable transport over metallic media.

Yellow Alarm - An alarm signal sent back toward the source of a failed signal due to the presence of an AIS (may be used by APS equipment to initiate switching).

Zero Byte Time Slot Interchange (ZBTSI) - A technique used with the T carrier extended superframe format (ESF) in which an area in the ESF frame carries information about the location of all-zero bytes (eight consecutive “0”s) within the data stream.

Zero Code Suppression - The insertion of a “1” bit to prevent the transmission of eight or more consecutive “0” bits. Used primarily with T1 and related digital telephone company facilities, which require a minimum “1’s density” in order to keep the individual subchannels of a multiplexed, high speed facility active.

Zero-Bit Insertion - A technique used to achieve transparency in bit-oriented protocols. A zero is inserted into sequences of one bits that cause false flag direction.

Index

A

ACR (Available Cell Rate) . . . . 16 - 11
AIS (Alarm Indication Signal) . . . . 13 - 1
alarm control . . . . 8 - 81
Alarm Indication Signal (AIS) . . . . 13 - 1
alarms
    resetting . . . . 8 - 82
AMI
    commands not available running remotely . . . . 16 - 6
    example scripts . . . . 16 - 16
    remote interface and scripting . . . . 16 - 1
appendices
    channel usage in FORE ATM networks B - 1
    FORE SNMP statistics . . . . .C - 1
asx0 . . . . 8 - 74
ASX-200 SCP
    front panel . . . . 8 - 7
ATM backbone switches . . . . 8 - 2
ATM connection routing . . . . 8 - 83
    NSAP prefixes . . . . 8 - 84
    NSAP routing . . . . 8 - 84
    static routing . . . . 8 - 86
ATM Management Interface . . . . 16 - 1
ATM networks subview . . . . 6 - 6
Available Cell Rate (ACR) . . . . 16 - 11
awk program . . . . 10 - 16

B

bandwidth
    reserving on a path . . . . 9 - 25, 9 - 27
bandwidth overbooking on a port
    configuring . . . . 8 - 66
billing, network utilization . . . . 10 - 15
border switch
    disabling for PNNI . . . . 16 - 9
    displaying for PNNI . . . . 16 - 14
    enabling for PNNI . . . . 16 - 9
    PNNI . . . . 16 - 9
buffer overbooking on a port
    configuring . . . . 8 - 66

C

call records
    configuring . . . . .14 - 4, 14 - 5
    post processing . . . . 14 - 9
CBR . . . . 9 - 41
CDVT . . . . 9 - 47
Cell Delay Variation Tolerance (CDVT) . 9 - 47
Cell Loss Priority (CLP) bit . . . . 9 - 47
channel tool
    browse .9 - 5, 13 - 8
    browser options . . . . 9 - 8
    channel control . . . . 9 - 4
    confirmation dialog boxes . . . . 9 - 10
    filtering by path and channel type . 9 - 9
    moving columns . . . . 9 - 11
    p-mp and mp-p confirmation dialog boxes . . . . 9 - 10
    sorting . . . . 9 - 10
    tool types . . . . 9 - 4
channel trace . . . . 11 - 1
    cell loss . . . . 11 - 7
    cell rejection . . . . 11 - 2
    cell throughput . . . . 11 - 2

channel utilization . . . . 11 - 2
contract bandwidth . . . . 11 - 9
droppage . . . . 11 - 2
host connection . . . . 11 - 3
inter-switch link . . . . 11 - 3
more than one link . . . . 11 - 3
number of hops . . . . 11 - 4
on a link . . . . 11 - 3
on a switch . . . . 11 - 3
overutilization . . . . 11 - 7
policing bandwidth . . . . 11 - 9
tabular . . . . 11 - 4
channel usage in FORE ATM networks . . B - 1
Classical IP interfaces . . . . 8 - 74
CLP bit . . . . 9 - 47
configuring and monitoring network modules . . . . 8 - 68
configuring and monitoring ports . . . . . . 8 - 15
DS-1 . . . . 8 - 34
DS-3 . . . . 8 - 29
E-1 . . . . 8 - 43
E-3 . . . . 8 - 38
generic . . . . 8 - 16
J-2 . . . . 8 - 48
OC-3 and OC-12 (SONET) . . . . 8 - 23
TP-25 . . . . 8 - 51
traffic . . . . 8 - 61
Constant Bit Rate (CBR) . . . . 9 - 41

D

display LED . . . . 8 - 7
reading ATM Switch . . . . 8 - 7
dropping cells . . . . 9 - 47
dual SCPs
configuring the controlling SCP . . 8 - 98
dual SCP mode . . . . 8 - 96
SCP heartbeat . . . . 8 - 96

E

Ethernet 10BaseT port . . . . 8 - 7
Ethernet interface . . . . 8 - 74

F

ForeThought PNNI SPVCs . . . . .9 - 2, 9 - 9
ForeView configuration . . . . 3 - 1
alternate discovery . . . . 3 - 3
configuration template . . . . 3 - 18
configuring SNMP . . . . 3 - 7
displaying reserved channels . . . . . 3 - 5
enclosure id name mapping . . . . . . 3 - 6
general format . . . . 3 - 2
graph type . . . . 3 - 5
maximum points to display . . . . 3 - 5
overview . . . . 3 - 1
PC directory file . . . . 3 - 2
seed switches . . . . 3 - 3
stand-alone map display order . . . . 3 - 4
stand-alone map NNIs . . . . 3 - 4
status polling . . . . 3 - 5
switch order . . . . 3 - 3
Unix directory file . . . . 3 - 2
ForeView stand-alone network map
default map . . . . 7 - 3
device labels . . . . 7 - 5
exploded view . . . . 7 - 4
launching ForeView tools . . . . 7 - 6
limiting network discovery . . . . 7 - 2
menu controls and commands . . . . 7 - 6
minimum requirements to run . . . . 7 - 2
navigating the map . . . . 7 - 9
nodes and connections . . . . 7 - 4
Windows NT configuration file . . . 7 - 2
Front Panel . . . . 8 - 1
ASX-200BX . . . . 8 - 5
configure menu . . . . 8 - 11
configuring and monitoring ports 8 - 15

menu bar . . . . 8 - 11, 13 - 7
network modules . . . . 8 - 8
polling . . . . 8 - 13, 13 - 7
port indicators . . . . 8 - 9
tachometers . . . . 8 - 12
VCCs (channel tool) . . . . 8 - 14
front panel
MSC-900 . . . . 8 - 3
TNX-1100 . . . . 8 - 4
TNX-210 . . . . 8 - 4

G

GCRA . . . . 9 - 47
Generic Cell Rate Algorithm (GCRA) . . . 9 - 47
graphing host usage . . . . 10 - 3, 10 - 8
graphing network usage . . . . 10 - 2

H

hardware
ASX-1000 . . . . 8 - 2
ASX-200 . . . . 8 - 6
ASX-200BX . . . . 8 - 3
ASX-200WG . . . . 8 - 5
hello indication messages . . . . 16 - 10
displaying the interval between . 16 - 13
setting the interval between . . . . . 16 - 10
HP OpenView
ATM networks submap . . . . 5 - 5
fvovmon . . . . 5 - 3, 5 - 14
fvovtrapd . . . . 5 - 3, 5 - 14
host usage, graphing . . . . 5 - 17
interswitch connections . . . . 5 - 5, 5 - 10
IP hostname . . . . 5 - 13
launching ForeView tools . . . . 5 - 16
link status . . . . 5 - 9
link status, host . . . . 5 - 9
map format . . . . 5 - 4
map icons . . . . 5 - 13
root level map . . . . 5 - 4
SNMP set messages . . . . 5 - 15
SNMP traps . . . . 5 - 15
switch connections submap . . . . 5 - 6
switch fabrics submap . . . . 5 - 9
threshold events . . . . 5 - 20

I

ie0 . . . . 8 - 74
installation . . . . 2 - 1
inventory . . . . 12 - 1
filtering by device or host type . . . 12 - 5
filtering by names and versions . . 12 - 5
filtering options . . . . 12 - 4
launching the inventory utility . . . 12 - 1
moving columns . . . . 12 - 7
options . . . . 12 - 3
sort decreasing option . . . . 12 - 3
sort order . . . . 12 - 6
sorting . . . . 12 - 6
IP addressing . . . . 8 - 73
IP configuration . . . . 8 - 72
IP forwarding
configuring . . . . 8 - 74
IP routing . . . . 8 - 76

L

leaky bucket algorithm . . . . 9 - 47
logging network usage . . . . 10 - 8
logging output . . . . 10 - 13
accounting information . . . . 10 - 14
databases . . . . 10 - 14
spreadsheets . . . . 10 - 14
login
serial port . . . . 16 - 3
telnet . . . . 16 - 4

M

Maximum Burst Size (MBS) . . . . . .9 - 41, 9 - 47

maximum hop count
displaying . . . . 16 - 13
setting . . . . 16 - 11
MBS . . . . 9 - 41, 9 - 43, 9 - 47
minimum threshold for NSAP updates
displaying . . . . 16 - 13
setting . . . . 16 - 12

N
network modules . . . . 8 - 8
port numbering . . . . 8 - 8
series C . . . . 8 - 61
series D . . . . 8 - 61
series LC . . . . 8 - 64
network utilization, billing . . . . 10 - 15
NEXT pushbutton . . . . 8 - 7
NSAP indication messages . . . . 16 - 10
displaying the interval between . 16 - 13
setting the interval between . . . . 16 - 10
NSAP prefix
creating . . . . 16 - 8
displaying . . . . 16 - 13
NSAP prefix mask for PNNI
displaying . . . . 16 - 13
setting . . . . 16 - 9

O
OAM cell generation
disabling . . . . 13 - 2
originating path . . . . 9 - 26
originating paths . . . . A - 6
overbooking . . . . 8 - 66

P
partial fill . . . . 9 - 15
PCR . . . . .9 - 41, 9 - 47
Peak Cell Rate (PCR) . . . . .9 - 41, 9 - 47
peergroup mask for PNNI
displaying . . . . 16 - 13
setting . . . . 16 - 10
performance monitoring
configuring . . . . .14 - 4, 14 - 5
PNNI SPVCs . . . . .9 - 2, 9 - 9
disabling rerouting . . . . .8 - 94, 9 - 23
enabling rerouting . . . . 9 - 23
pacing . . . . 8 - 93
PNNI topology . . . . 16 - 8
point-to-multipoint connections (PMPs) 8 - 92
power LED . . . . 8 - 7
proportional multiplier
displaying . . . . 16 - 13
setting . . . . 16 - 11

Q
qaa0 . . . . 8 - 74
qaa1 . . . . 8 - 74
qaa2 . . . . 8 - 74
qaa3 . . . . 8 - 74

R
RDI (Remote Defect Indication) . . . . 13 - 1
re-installing . . . . 2 - 1
Remote Defect Indication (RDI) . . . . 13 - 1
reserved channels . . . . B - 1
RESET button . . . . 8 - 7

S
SCR . . . . .9 - 41, 9 - 47
SELECT pushbutton . . . . 8 - 7
serial port . . . . 8 - 7
signalling . . . . 8 - 78
Smart Permanent Virtual Circuit . 9 - 12, A - 10
SNMP . . . . 3 - 7
aligning SNMP configuration with
HP OpenView SNMP configuration 3 - 7
community names . . . . 3 - 7
SNMP indexing . . . . C - 1
SNMP trap . . . . .D - 1

supported on the switch . . . . .D - 1
software installation . . . . 2 - 1
Windows NT . . . . 2 - 10
software license key . . . . 2 - 6
software manager
requirements . . . . 15 - 1
upgrading switch software . . . . . . 15 - 1
SPANS interface . . . . 8 - 74
SPVC (Smart Permanent Virtual Circuit) .9 - 12, A - 10
SRTS (Synchronous Residual Time Stamp) . . . . 9 - 15
static route update indication messages 16 - 11
displaying the interval between . 16 - 13
setting the interval between . . . . . 16 - 11
SunNet Manager
ATM network status . . . . 6 - 15
ATM networks view . . . . 6 - 6
device labels . . . . 6 - 9
error logs . . . . 6 - 19
home view . . . . 6 - 5
initializing the database . . . . 6 - 3
interswitch links . . . . 6 - 7
launching ForeView tools . . . . 6 - 11
monitoring the ATM network . . . . 6 - 16
problems receiving traps . . . . 6 - 19
problems with discovery . . . . 6 - 19
re-discovering the network . . . . . . 6 - 18
running ForeView Discovery . . . . . 6 - 4
SNMP traps . . . . 6 - 17
starting ForeView . . . . 6 - 2
switch connections view . . . . 6 - 8
switch subnet glyphs . . . . 6 - 7
troubleshooting ForeView . . . . 6 - 19
update properties . . . . 6 - 17
Sustainable Cell Rate (SCR) . . . . . 9 - 41, 9 - 47
switch connections subview . . . . 6 - 8
switch control processor . . . . 8 - 7
switch software upgrade
obtaining the upgrade
via ftp . . . . 2 - 2
Synchronous Residual Time Stamp (SRTS) . . . . 9 - 15
system requirements . . . . 1 - 12

T

tagging cells . . . . 9 - 47
temperature sensors . . . . 8 - 81
terminate logging . . . . 10 - 12
terminating path . . . . 9 - 24
terminating paths . . . . .A - 6
through paths . . . . .A - 4
topology scripts . . . . 16 - 14
traffic policing . . . . .8 - 61, 9 - 41
traps . . . . 6 - 17

U

UBR . . . . 9 - 41
Unspecified Bit Rate (UBR) . . . . 9 - 41
UPC . . . . 9 - 41
UPC traffic contract parameters . . . . 9 - 48
Usage Parameter Control (UPC) . .9 - 41, 9 - 47

V

Variable Bit Rate (VBR) . . . . 9 - 41
VBR . . . . 9 - 41
vcmark
displaying . . . . 16 - 13
setting . . . . 16 - 12
virtual channel . . . . .A - 7
virtual channel identifier (VCI) . . . . .A - 1
virtual path . . . . .A - 3
virtual path identifier (VPI) . . . . .A - 1
virtual path terminators . . . . .A - 6

W

warranty . . . . 1 - 11

WindowsNT

starting the ForeView stand-alone network map . . . . 7 - 2